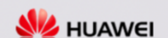
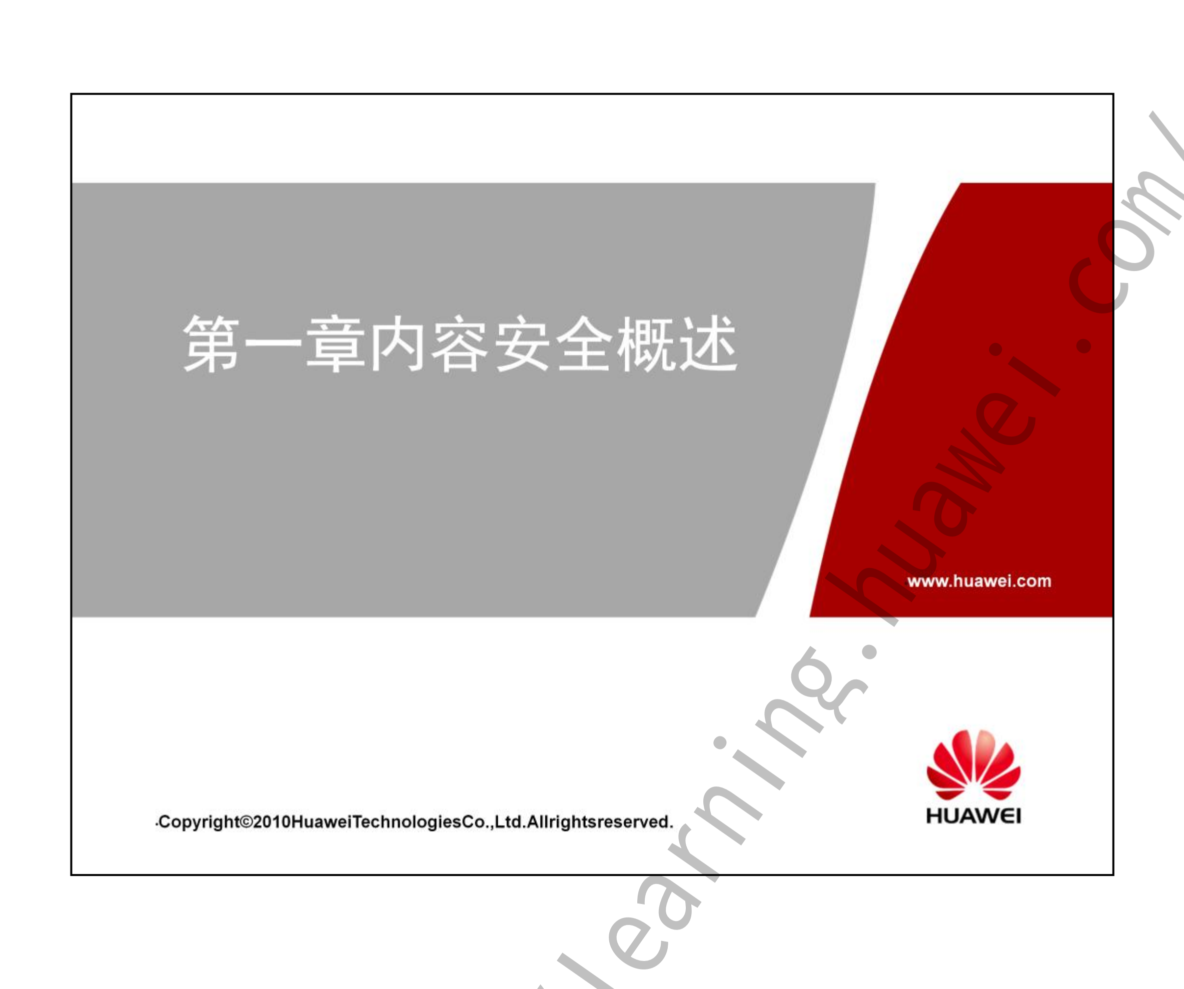
华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*) 享有如下特权：

- 1、**华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：请提交您的"华为账号"和注册账号的"email地址"到 *Learning@huawei.com 申请权限。*
- 2、**华为培训教材下载**
  - **内容**：**华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入"*华为培训->面授培训*"，在具体课程页面即可下载教材。
- 3、**华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见LVC排期：
    http://support.huawei.com/learning/NavigationAction!createNavi#navi[id]=_16
- 4、**学习工具 eNSP**
  - *eNSP (Enterprise Network Simulation Platform),* 是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。（http://support.huawei.com/ecommunity/bbs/list_2247.html ）




第一章内容安全概述
www.huawei.com
HUAWEI
·Copyright©2010HuaweiTechnologiesCo.,Ltd.Allrightsreserved.



目标

- 学完本课程后，您将能够:
  - 了解信息安全的基础知识；
  - 了解内容安全产生的背景；
  - 了解内容安全主要技术。





目录



信息安全概念

- 什么是信息?
  - 一般意义：信息是指事物运动的状态和方式，一种属性。
  - ISO/IEC-IT安全管理指南：信息是通过在数据上施加某些约定而赋予的这些数据特定的含义。
- 信息是无形的，可以通过各种媒介存储和传输。
- IT领域:信息是一种资产，包括信息本身（数据、文件、专利等）及信息存储和传输的介质（计算机、网络及设备等）。



- 信息就是对客观事物的反映，从本质上看信息是对社会、自然界的事物特征、现象、本质及规律的描述；
- 信息所描述的内容是通过某种载体如符号、声音、文字、图形、图象等来表征和传播的；
- 信息处理主要包括：信息的收集、信息的输入、信息的加工、信息的输出、信息的存储和传输。



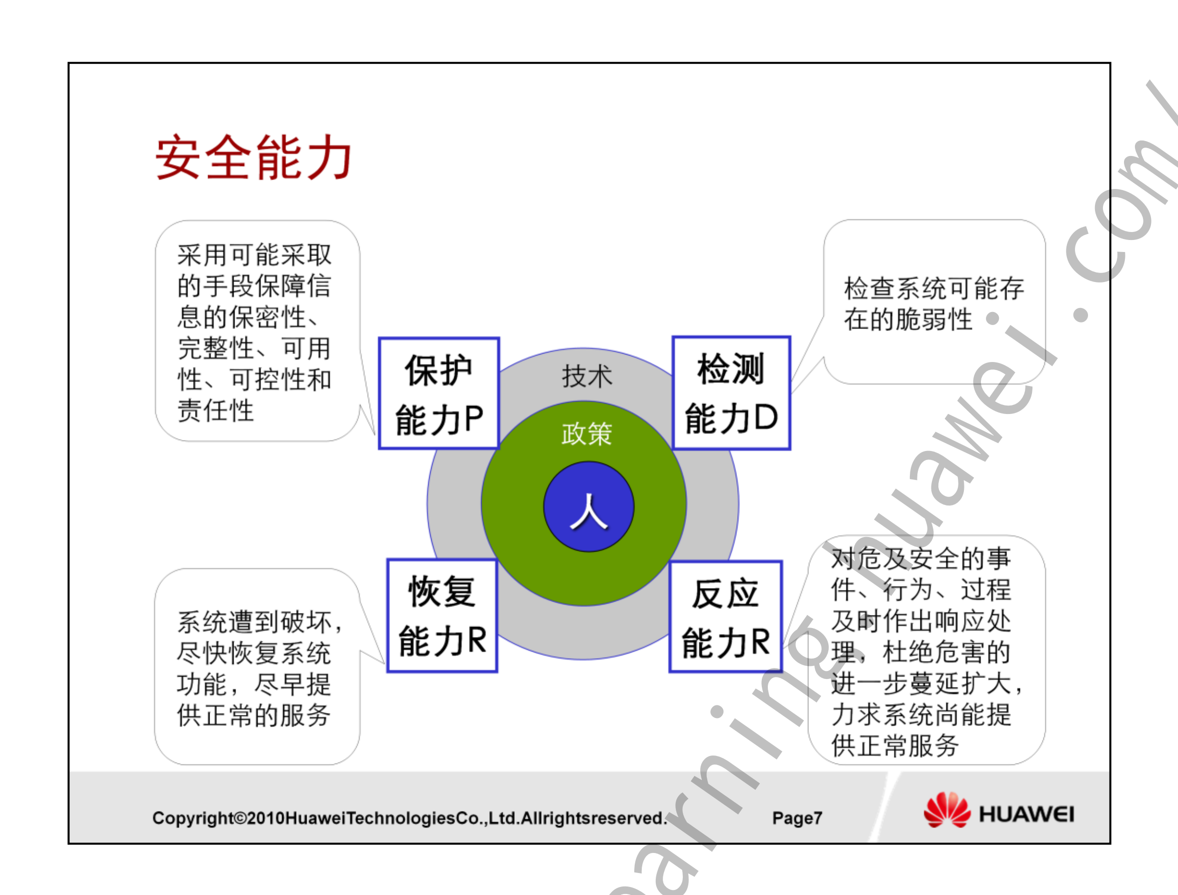
- 信息安全包括以下几个方面：
  - 保密性：Confidentiality--确保信息只能由那些被授权使用的人获取；
  - 完整性：Integrity--保护信息及其处理方法的准确性和完整性；
  - 可用性：Availability--确保被授权使用人在需要时可以获取信息和使用相关的资产；
  - 可控性：Controllability--对信息和信息系统实施安全监控管理，防止非法利用信息和信息系统；
  - 不可抵赖性：Non-Repudiation--防止信息源用户对他发送的信息事后不承认,或者用户接收到信息之后不认帐。

信息安全涉及到信息的保密性、完整性、可用性、可控性和不可抵赖性，总体来看,就是要保障信息的有效性。



安全需求的层次可以分为法规顺从，这是基于法律层面的，还有物理安全、接入安全、传输安全及存储安全和使用安全等等。

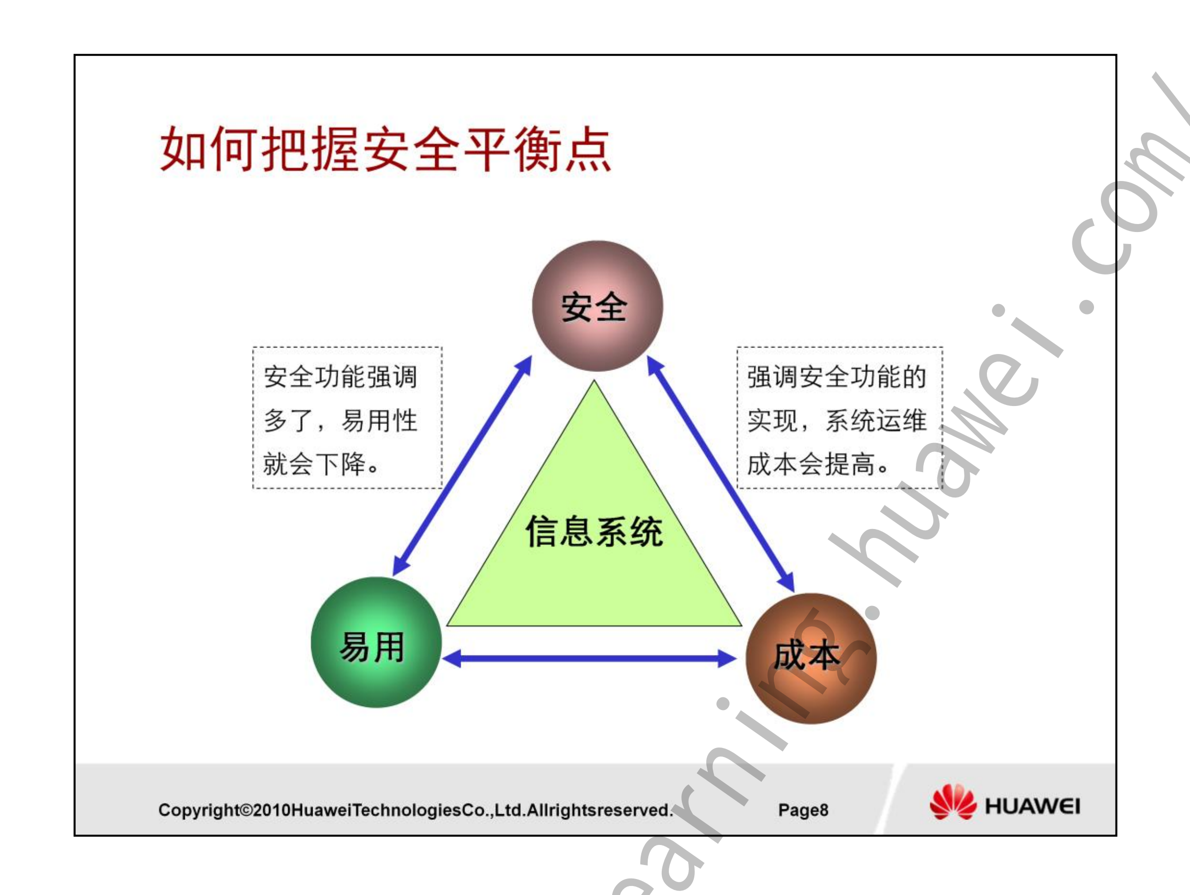
依据不同的安全考虑需求可能划分的层次不一样。这里主要从网络安全的角度侧重于物理安全、接入安全和内部及节点安全。业务信息的安全通过使用相关的技术手段来提高安全性。



安全因素都涉及到人。在现在的安全因素中，安全的管理能力显得特别重要，因为信息最终都是由人去处理，对能接触信息的人安全管理不严的话，其它的任何的技术都是白搭。在安全管理政策及策略下，再通过相关的技术手段来提高安全的能力。

- 安全能力可以分为四种：
  - Protection(防护)；
  - Detection(检测)；
  - Response(响应)；
  - Recovery(恢复)。

目前比较普遍的讲的安全模型是PDRR安全模型。



安全、易用与成本之间的关系是一个三角的关系，要取得一个很好的落足点不容易。安全的功能强调多了，系统的易用性就会下降，同时实现安全功能，维护安全系统的成本就上去了，如果降低相关的安全要求，那就得面临因可能爆发的安全问题而引发的其它成本。

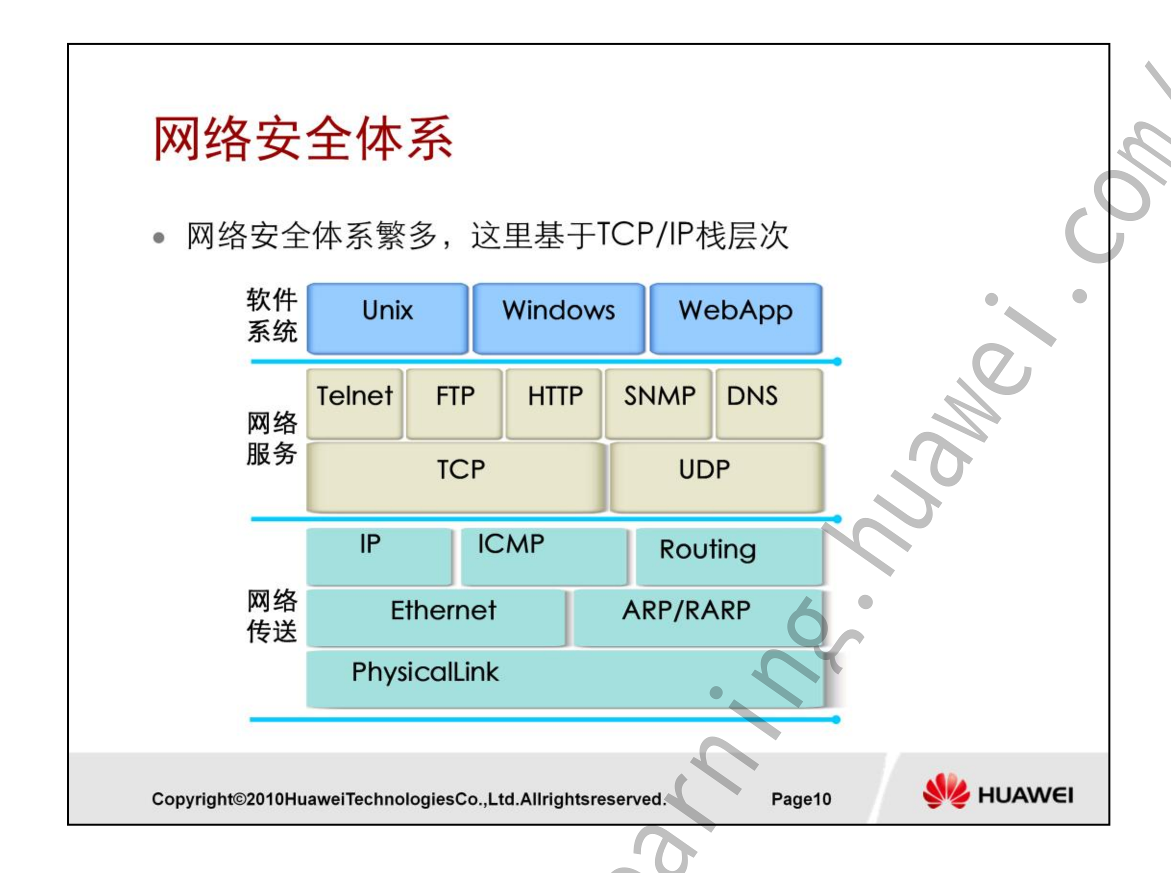
安全是一项耗费时间，又耗费资源的工作，必须根据不同的产品或项目来把握其与易用、成本之间的平衡关系。

- 产品在安全上考虑的越多，那么就很可能导致其性能的下降；
- 安全上考虑的越多，那么其安装维护的复杂度会增加、操作使用的便利性会减少；
- 产品在安全上考虑的越多，那么其可靠性往往会得到增加，一方面是减少了各类黑客攻击，二是产品自身的可靠性保障会得到更多的考虑；
- 安全性提升意味着产品研发成本提高、产品开发周期增长，前期投入和后期维护成本也会增加，这些成本最终都转嫁到用户成本上；
- 由于安全性得到增强，安全事故成本会减少，给用户造成的经济、信誉损失会减少。



目录





- 网络安全体系繁多，这里就依据TCP/IP的协议栈层次关系来进行分析；
- 了解网络当中常见的安全风险并掌握降低风险的措施是很有必要的；
- TCP/IP的层次分为两大块，并另外加上一层软件系统，可以从三个层面来进行分析。

TCP/IP协议栈与常见安全风险

应用层	缓冲区溢出，漏洞，病毒、木马、CC攻击等
传输层	TCP欺骗，UDP欺骗，TCPSYNFlood，TCPFlag等
网络层	路由攻击，IP欺骗，泛洪攻击，报文分片等
链路层	Mac欺骗，Mac泛洪，ARP欺骗等
物理层	设备破坏，线路侦听



网络上的各种攻击类型很多，攻击的目的也不同，有的是为了破坏中断服务，有的是为了窃取信息等不一而足。

- 基于物理层的攻击；
- 基于链路层的攻击，在内网上基于链路层的攻击较常见；
- 网络层的攻击包括一些泛洪攻击、Dos攻击等；
- 传输层包括两大块，利用TCP的攻击和利用UDP的攻击；
- 应用层含有很多目前各大网站所关注的攻击类型，包括缓冲区溢出，操作系统或软件系统漏洞攻击，以及病毒攻击，木马攻击等等。



目录



安全威胁分析

- 网络威胁
  - 黑客入侵、拒绝服务攻击、病毒及恶意软件、个人安全意识薄弱
- 网络威胁的现状
  - 现在大多数病毒等网络威胁不再单纯地攻击电脑系统，而是被黑客攻击和不法分子利用，成为他们获取利益的工具。因此，传统的电脑病毒等网络威胁，正在向由利益驱动的、全面的网络威胁发展变化。

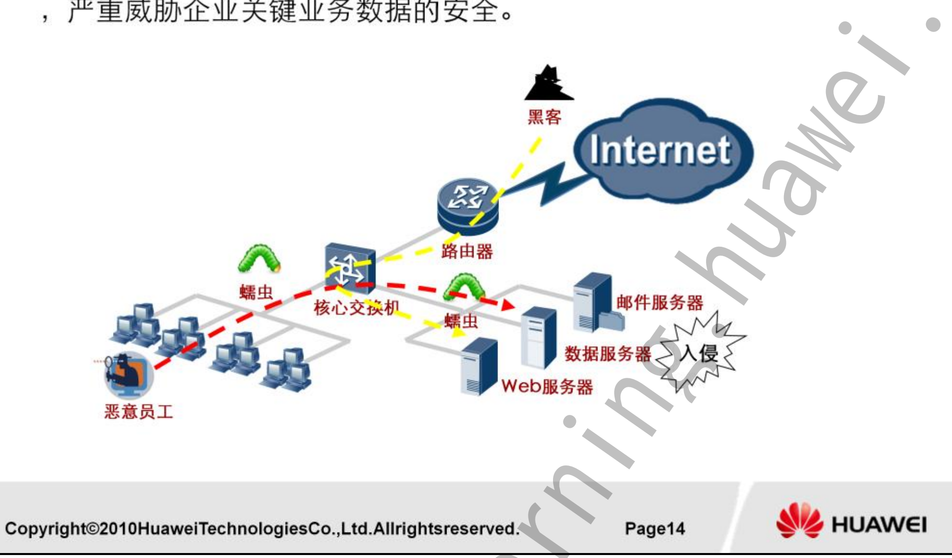


在目前出现的各种安全威胁当中，恶意程序（病毒与蠕虫、Bot、Rootkit、特洛依木马与后门程序、弱点攻击程序以及行动装置恶意程序）类别占有很高的比例，灰色软件（间谍/广告软件）的影响也逐渐扩大，而与犯罪程序有关的安全威胁已经成为威胁网络安全的重要因素。

目前用户面临的不再是传统的病毒攻击，“网络威胁”经常是融合了病毒、黑客攻击、木马、僵尸、间谍等危害等于一身的混合体，因此单靠以往的防毒或者防黑技术往往难以抵御。

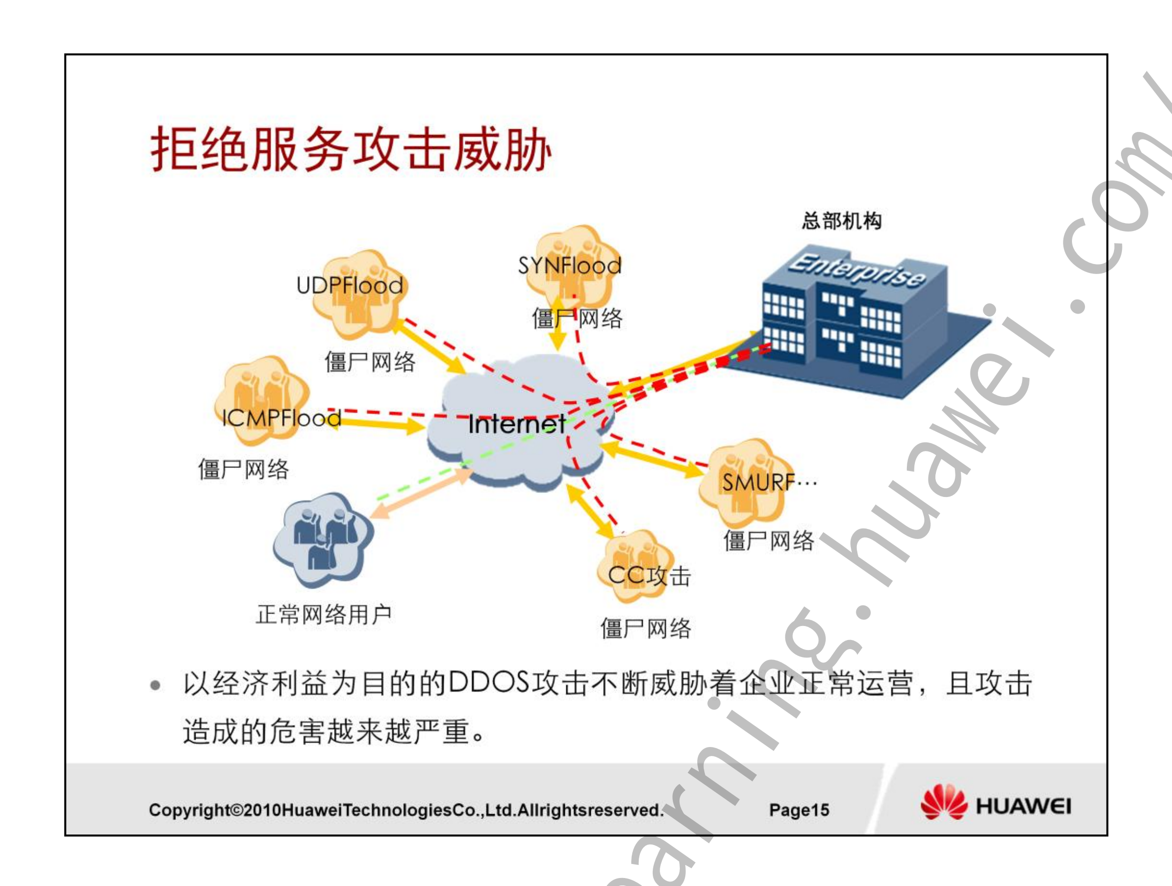
黑客入侵

- 网络黑客、企业内部恶意员工利用系统及软件的漏洞，入侵服务器，严重威胁企业关键业务数据的安全。

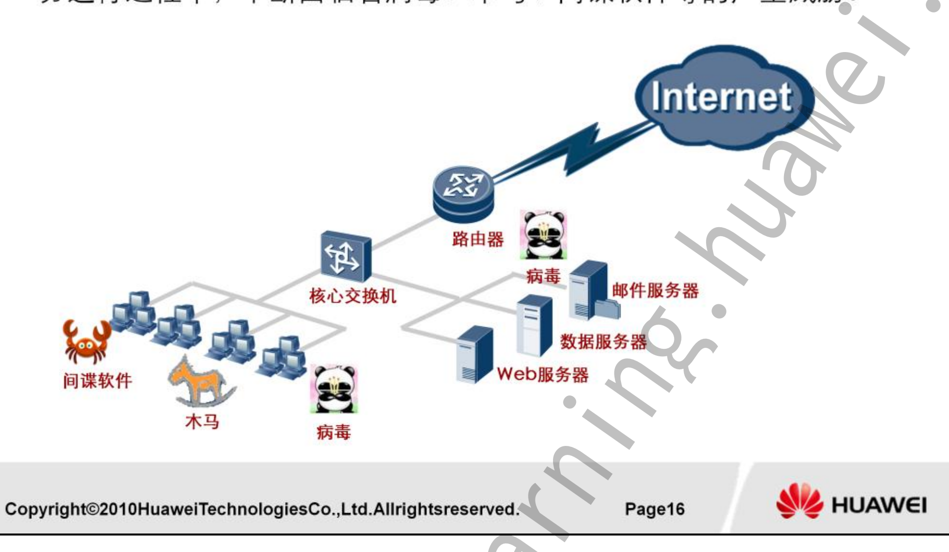


服务器漏洞给企业造成严重的安全威胁：

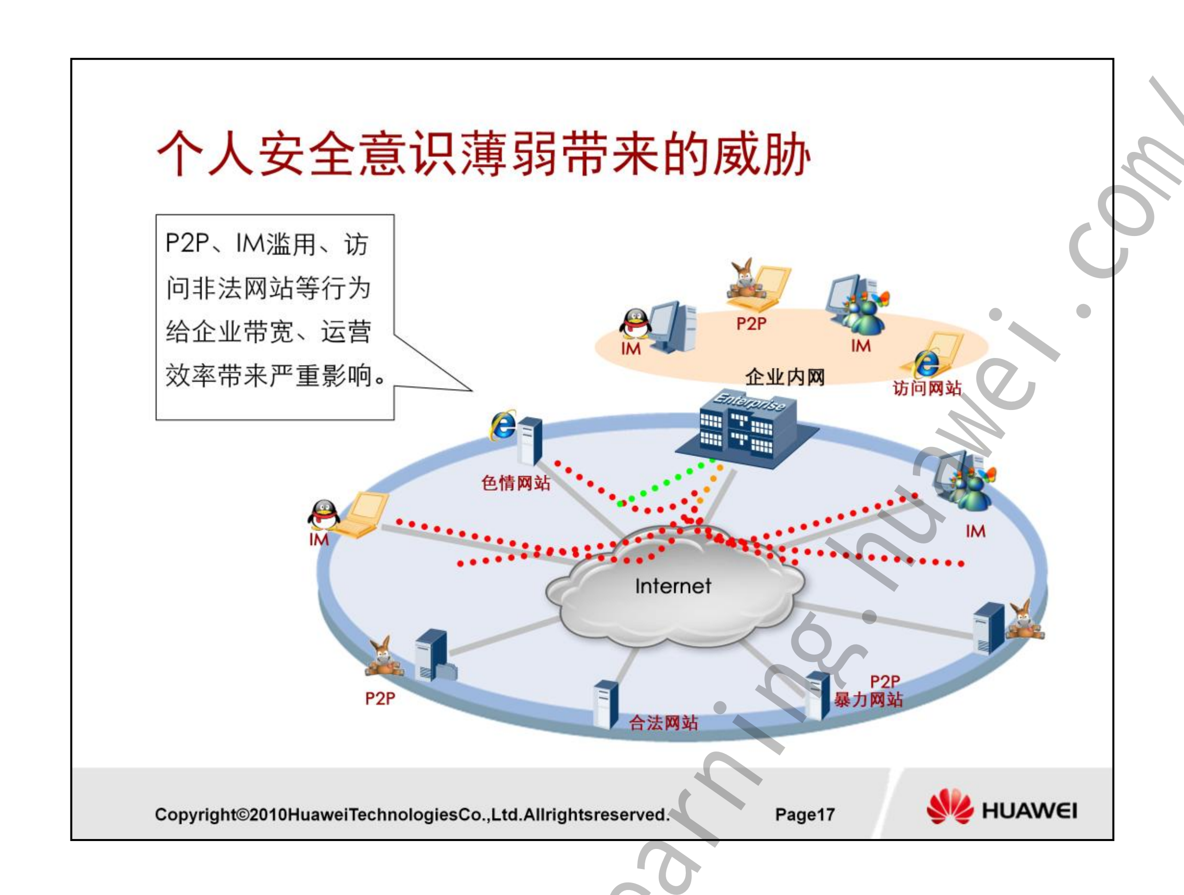
- 企业内网中许多应用软件可能存在漏洞；
- 互联网使应用软件的漏洞迅速传播；
- 蠕虫利用应用软件漏洞大肆传播，消耗网络带宽，破坏重要数据；
- 黑客、恶意员工利用漏洞攻击或入侵企业服务器，业务机密被篡改、破坏和偷窃。



- DDOS攻击威胁:
  - 以经济利益为目标的全球黑色产业链的形成，网络上存在大量僵尸网络;
  - 不法分子的敲诈勒索，同行的恶意竞争等都有可能导致企业遭受DDoS攻击;
  - 遭受DDoS攻击时，网络带宽被大量占用，网络陷于瘫痪；受攻击服务器资源被耗尽无法响应正常用户请求，严重时会造成系统死机，企业业务无法正常运行。



- 浏览网页、邮件传输是病毒、木马、间谍软件进入内网的主要途径；
- 病毒能够破坏计算机系统，篡改、损坏业务数据；
- 木马使黑客不仅可以窃取计算机上的重要信息，还可以对内网计算机破坏；间谍软件搜集、使用、并散播企业员工的敏感信息，严重干扰企业的正常业务；
- 桌面型反病毒软件难于从全局上防止病毒泛滥。



- P2P、IM滥用给企业带宽、运营效率带来严重影响。员工不受控Web访问可能会:
  - 被不安全的链接或者恶意下载植入代码，使机构成为僵尸网络或者感染病毒;
  - 容易被含有欺骗信息的钓鱼网站所欺骗，泄露个人银行帐号、密码等机密信息;
  - 被娱乐性内容所吸引;
  - 网页中可能带有与法律相抵触的内容（如色情、暴力），给企业带来一系列法律风险。



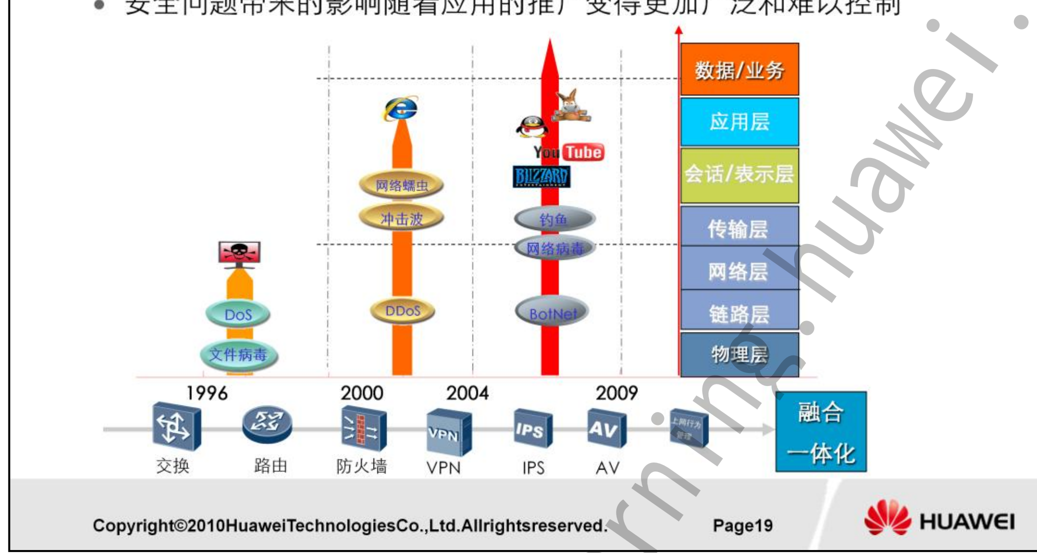
目录

1. 信息安全基础知识
2. **内容安全产生背景**

   2.1安全威胁分析

   2.2安全发展趋势
3. 内容安全技术简介





攻击从网络层向应用及业务层延伸，要求以网络为核心的TM技术和以终端为核心的SCM技术在网络上进行融合防范；

对资源及内容的优化管理成为最关心的主题—对SA的需求，以SA技术为核心的业务应用将成为重点；

客户从设备需求到服务需求的转化，SCTM/SA等产品的应用要求持续提供升级及响应服务，使得商业模式发生演化；

从网络安全向安全网络转化，芯片、软件技术的发展使得网络产品和安全产品的融合成为可能，广域网安全、多台网关设备集中管理、TCO等需求必将驱使路由器与安全产品融合，建设安全的网络成为基本要求。

病毒的发展趋势

- 病毒与黑客程序相结合
  - 随着网络业务的普及和互动的增多，病毒与黑客程序（木马病毒）结合以后的危害更为严重。
- 蠕虫病毒更加泛滥，木马、僵尸已成为主流
- 病毒破坏性更大
  - 计算机病毒不再仅仅以侵占和破坏单机的资料为目的；
  - 混合型病毒的传播速度非常快，其造成的破坏程度也要比以前的计算机病毒所造成的破坏大得多。



- 当今的网络时代，病毒的发展更呈现出以下趋势：
  - 病毒与黑客程序相结合，随着网络业务的普及和互动的增多，病毒与黑客程序（木马病毒）结合以后的危害更为严重。
  - 蠕虫病毒更加泛滥，木马、僵尸已成为主流
  - 病毒破坏性更大

计算机病毒不再仅仅以侵占和破坏单机的资料为目的。木马病毒的传播使得病毒在发作的时候有可能自动联络病毒的创造者（如爱虫病毒），或者采取DoS（拒绝服务）的攻击（如红色代码病毒）。一方面可能会导致本机机密资料的泄漏，另一方面会导致一些网络服务的中止。而蠕虫病毒则会抢占有限的网络资源，造成网络堵塞（如Nimda病毒）。如有可能，还会破坏本地的资料（如针对911恐怖事件的Vote病毒）。

具备这些特征的病毒被称为混合型病毒，混合型病毒的传播速度非常快，其造成的破坏程度也要比以前的计算机病毒所造成的破坏大得多。混合型病毒的出现使人们意识到有必要设计一个有效的保护战略，而不是一个单独的产品来对病毒进行防护。

网络攻击的新趋势

- 攻击过程的自动化与攻击工具的快速更新
  - 扫描潜在的受害者
  - 入侵具有漏洞的系统
  - 攻击扩散
  - 攻击工具的协同管理
- 攻击工具的不断复杂化
  - 反检测
  - 动态行为
  - 攻击工具的模块化
- 漏洞发现得更快
- 渗透防火墙



- 趋势一：攻击过程的自动化与攻击工具的快速更新

攻击工具已经将对漏洞的入侵设计成为扫描活动的一部分，这样大大加快了入侵的速度。2000年之前，攻击工具需要一个人来发起其余的攻击过程。现在，攻击工具能够自动发起新的攻击过程。例如红色代码和Nimda病毒这些工具就在18个小时之内传遍了全球。随着分布式攻击工具的产生，攻击者能够对大量分布在Internet之上的攻击工具发起攻击。现在，攻击者能够更加有效地发起一个分布式拒绝服务攻击。

- 趋势二：攻击工具的不断复杂化

攻击工具的编写者采用了比以前更加先进的技术。攻击工具的特征码越来越难以通过分析来发现，并且越来越难以通过基于特征码的检测系统发现。

- 趋势三：漏洞发现得更快

随着发现漏洞的工具的自动化趋势，留给用户打补丁的时间越来越短。尤其是缓冲区溢出类型的漏洞，其危害性非常大而又无处不在，是计算机安全的最大的威胁。在CERT和其它国际性网络安全机构的调查中，这种类型的漏洞是对服务器造成后果最严重的。

- 趋势四：渗透防火墙

我们常常依赖防火墙提供一个安全的主要边界保护，但目前已经存在一些绕过典型防火墙配置的技术，如IPP（the Internet Printing Protocol）和Web DAV（Web-based Distributed Authoring and Versioning）；一些标榜是“防火墙适用”的协议实际上设计为能够绕过典型防火墙的配置；特定特征的"移动代码"（如ActiveX控件，Java和Java Script）使得保护存在漏洞的系统以及发现恶意的软件更加困难。

安全产品的发展趋势

- 以传统防火墙为载体，各种安全技术实现多维度的融合。安全产品发展表现出以下趋势:
  - 高性能、大容量
  - 深度检测，全面过滤木马、垃圾邮件、病毒等等
  - 支持IPv6，适应未来的网络
  - 集成IDS/IPS
  - 分布式
  - 嵌入式防火墙
  - 多功能、多业务能力



日益提高的安全需求对信息安全产品提出了越来越高的要求，本文重点针对防火墙产品的主要发展趋势。

- 模式转变

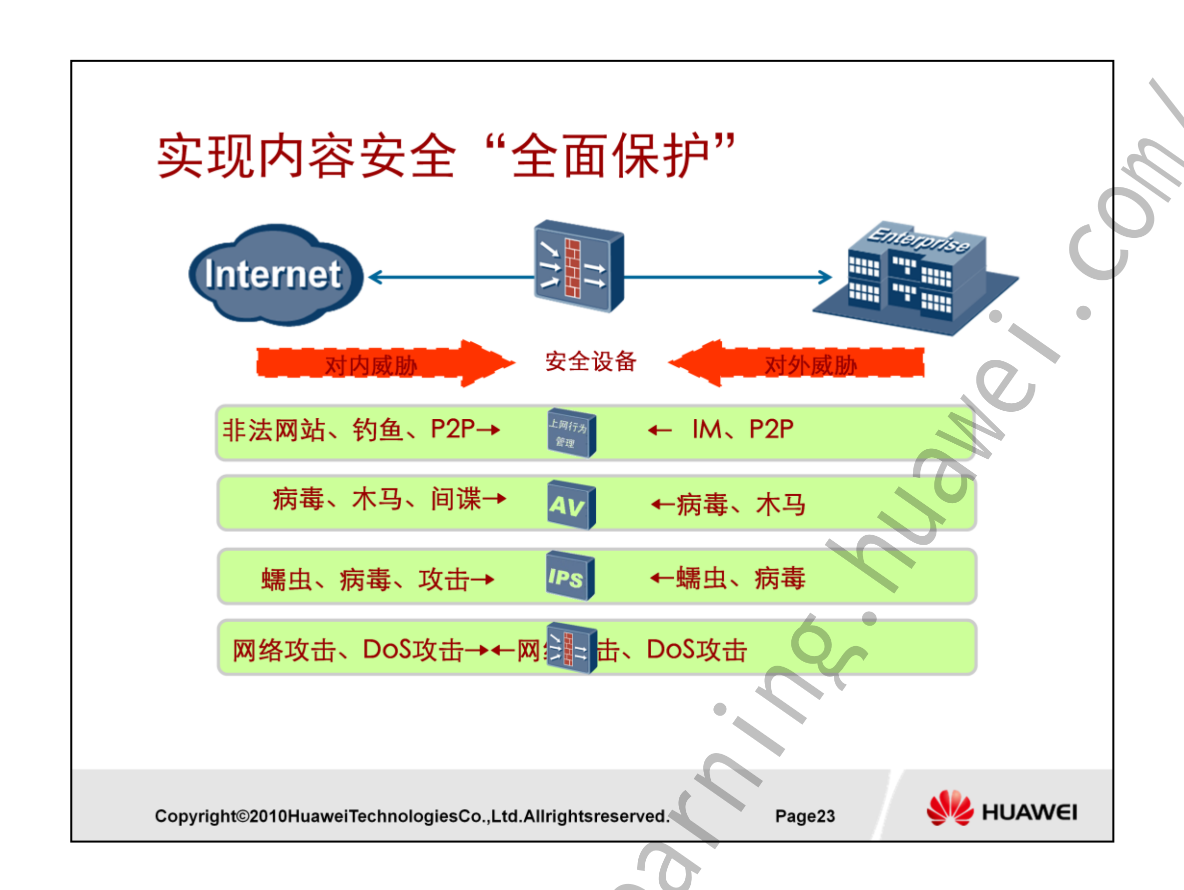
传统的防火墙通常都设置在网络的边界位置，不论是内网与外网的边界，还是内网中的不同子网的边界，对数据流进行分隔，形成安全管理区域。现在越来越多的防火墙产品也开始体现出一种分布式结构，以分布式为体系进行设计的防火墙产品以网络节点为保护对象，可以最大限度地覆盖需要保护的对象，大大提升安全防护强度。目前较为先进的一种过滤方式是带有状态检测功能的数据包过滤，其实这已经成为现有防火墙产品的一种主流检测模式，可以预见，未来的防火墙检测模式将继续整合进更多的范畴。

- 功能扩展

现在的防火墙产品已经呈现出一种集成多种功能的设计趋势，包括VPN、AAA、PKI、IPSec等附加功能，甚至防病毒、入侵检测这样的主流功能，都被集成到防火墙产品中了，很多时候我们已经无法分辨这样的产品到底是以防火墙为主，还是以某个功能为主了，即其已经逐渐向我们普遍称之为IPS（入侵防御系统）的产品转化了。防火墙的管理功能一直在迅猛发展，并且不断地提供一些方便好用的功能给管理员，这种趋势仍将继续，更多新颖实效的管理功能会不断地涌现出来。

- 性能提高

未来的防火墙产品由于在功能性上的扩展，以及应用日益丰富、流量日益复杂所提出的更多性能要求，会呈现出更强的处理性能要求。



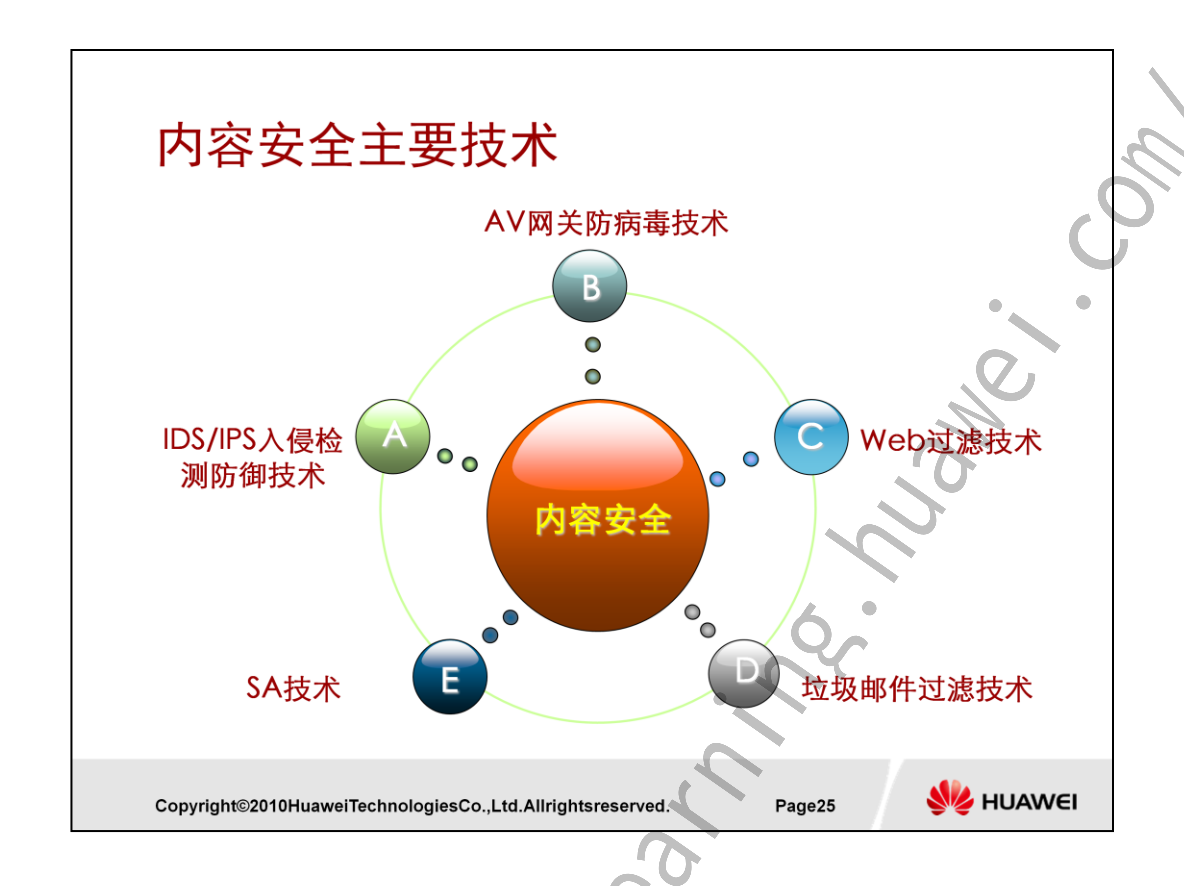
华为公司的USG5000系列安全产品融合了上网行为管理、AV网关防病毒、IPS入侵防御系统、防DDOS攻击等特性，为更好的解决来自企业内部、外部的攻击威胁提供了强有力的保障。

AV防护的是病毒文件,如邮件的附件，通过HTTP方式下载的文件中含有病毒等。IPS防护的是病毒的一些攻击行为，如蠕虫的自我传播。



目录





- 入侵检测/防御技术（IDS/IPS）

入侵检测/防御技术是通过监视各种操作，分析、审计各种数据和现象来实时检测入侵行为的过程，它是一种积极的和动态的安全防御技术。

- 网关防病毒技术（AV）

利用病毒库和病毒引擎技术，保护网络，使其远离多种动态威胁，包括病毒、间谍软件、蠕虫、木马病毒、后门和其它恶意代码等。

- WEB过滤技术

包括阻止内部用户访问非法的网址，对网页内的Java或ActiveX程序进行阻断；恶意网页检测、识别等。

- 垃圾邮件过滤技术(SPAM)

通过对邮件服务系统的安全加固和垃圾邮件过滤技术解决日益扩大的垃圾邮件问题

- SA业务感知技术

通过对报文的应用层数据进行内容检测，分析报文或流在IP和UDP/TCP层以上及各种隧道内部的应用类型。

入侵检测/防御技术

- 入侵检测（ID，IntrusionDetection）
- 入侵检测系统（IDS，IntrusionDetectionSystem）
- 入侵防御系统（IPS，IntrusionPreventionSystem）



- 入侵检测（ID，IntrusionDetection）

  通过监视各种操作，分析、审计各种数据和现象来实时检测入侵行为的过程，它是一种积极的和动态的安全防御技术。

  入侵检测的内容涵盖了授权的和非授权的各种入侵行为，例如，违反安全策略行为、冒充其他用户、泄露系统资源、恶意行为、非法访问，以及授权者滥用权力等。

- 入侵检测系统（IDS，IntrusionDetectionSystem）

  用于入侵检测的所有软硬件系统。这个系统可以通过网络和计算机动态地搜集大量关键信息资料，并能及时分析和判断整个系统环境的目前状态，一旦发现有违反安全策略的行为或系统存在被攻击的痕迹等，立即启动有关安全机制进行应对，例如，通过控制台或电子邮件向网络安全管理员报告案情，立即中止入侵行为、关闭整个系统、断开网络连接等。

- 入侵防御系统（IPS，IntrusionPreventionSystem）

  发现入侵行为时能实时阻断的入侵检测系统。

网关防病毒技术

- 恶意代码
  - 是一种程序，它通过把代码在不被察觉的情况下镶嵌到另一段程序中，从而达到破坏被感染电脑数据、运行具有入侵性或破坏性的程序、破坏被感染电脑数据的安全性和完整性的目的。
- 病毒
  - 属于恶意代码，是附着于程序或文件中的一段计算机代码，以自我复制为明确目的，它可能损坏硬件、软件和信息。
- 病毒传播途径



- 电子邮件
  - HTML正文可能被嵌入恶意脚本；
  - 邮件附件携带病毒压缩文件；
  - 利用社会工程学进行伪装，增大病毒传播机会。
- 网络共享
  - 病毒会搜索本地网络中存在的共享，包括默认共享；
  - 通过空口令或弱口令猜测，获得完全访问权限，病毒自带口令猜测列表；
  - 将自身复制到网络共享文件夹中，通常以游戏,CDKEY等相关名字命名。
- P2P共享软件
  - 将自身复制到P2P共享文件夹，通常以游戏,CDKEY等相关名字命名；
  - 通过P2P软件共享给网络用户；
  - 利用社会工程学进行伪装，诱使用户下载。
- 系统漏洞
  - 由于操作系统固有的一些设计缺陷,导致被恶意用户通过畸形的方式利用后,可执行任意代码,这就是系统漏洞
  - 病毒往往利用系统漏洞进入系统,达到传播的目的。
- 其他常见病毒感染途径
  - 网页感染；
  - 与正常软件捆绑；
  - 用户直接运行病毒程序。

Web过滤技术

- 恶意网站安全威胁
- 恶意网站趋势
- 基础Web过滤技术
  - 网站地址过滤；
  - URL参数过滤；
  - Java/ActiveX阻断；
  - 恶意网站检测、识别。



恶意网页，是指网页的内容中被嵌入恶意代码，当用户访问恶意网页时，恶意代码被植入用户的计算机，可能会导致用户计算机上的隐私信息泄露，计算机成为僵尸网络等严重问题。

截止2009年底，华为安全能力中心已累计发现恶意网站156905个，占所有被监控网站数量的1.4%，这意味着，平均每100个网站中，就有1.4个网站曾经或正在被黑客攻击，成为恶意网站。

垃圾邮件过滤技术

- 垃圾邮件威胁
  - 垃圾邮件是指那些“违背收件者意愿”的邮件。有别于一般的正当商业广告邮件，垃圾邮件大多包含“反动、色情、暴力”信息，通过非法手段获取用户邮箱地址，对互联网资源和用户资源进行侵占和滥用
- 垃圾邮件危害
  - 带宽；
  - 资源；
  - 隐私；
  - 工作效率。
- 垃圾邮件过滤技术环节



- 垃圾邮件过滤技术--预防
  - 增强邮件服务器的安全性，防止漏洞及时补丁；
  - 提高系统防病毒能力；
  - 提供邮件服务安全身份认证；
  - 添加反垃圾邮件的专用设备或插件。
- 垃圾邮件过滤技术--检测
  - IP、域名、邮件地址的黑白名单及RBL方式；
  - SMTP通信链接速率、频度的设定；
  - 反向域名验证法；
  - 基于信头、信体、附件的内容关键词；
  - 基于贝叶斯算法的统计分析；
  - 基于垃圾邮件判定规则。
- 垃圾邮件过滤技术--响应
  - 丢弃(Drop)；
  - 标记（Lable）；
  - 隔离（Quarantine）。

深度报文检测技术

- 特征检测
- 关联识别
- 行为检测



- 特征检测

通过模式匹配算法，根据已知协议的内容特征，对网络报文的应用层内容进行匹配检索:单包匹配、多包匹配、多流匹配。

- 关联识别

对通讯控制通道和数据传输通道分开的应用协议，将多个通道流量进行协同检测；

对于某些业务类型已经判定的流量，可以通过三元组对与同一主机端口进行通讯的不同流量进行关联判断。

- 行为检测

通过分析各种应用的连接数、单IP的连接模式、上下行流量的比例、数据包发送频率等指标来区分应用类型。

入侵检测及防御技术、网关防病毒技术、WEB过滤技术、垃圾邮件过滤技术、深度业务监控技术的内容在后面各章节将详细说明。



总结

- 信息安全的基础知识
- 内容安全技术产生的背景
- 内容安全主要技术



练习题

- 判断题
  1. SA技术是通过对报文的应用层数据进行内容检测，分析报文或流在IP和UDP/TCP层以上及各种隧道内部的应用类型。
- 多选题
  1. 下列属于应用层常见的攻击有?

  A、缓冲区溢出B、病毒C、CC攻击D、arp欺骗网



习题与答案：

1、SA技术是通过对报文的应用层数据进行内容检测，分析报文或流在IP和UDP/TCP层以上及各种隧道内部的应用类型。

答案：正确

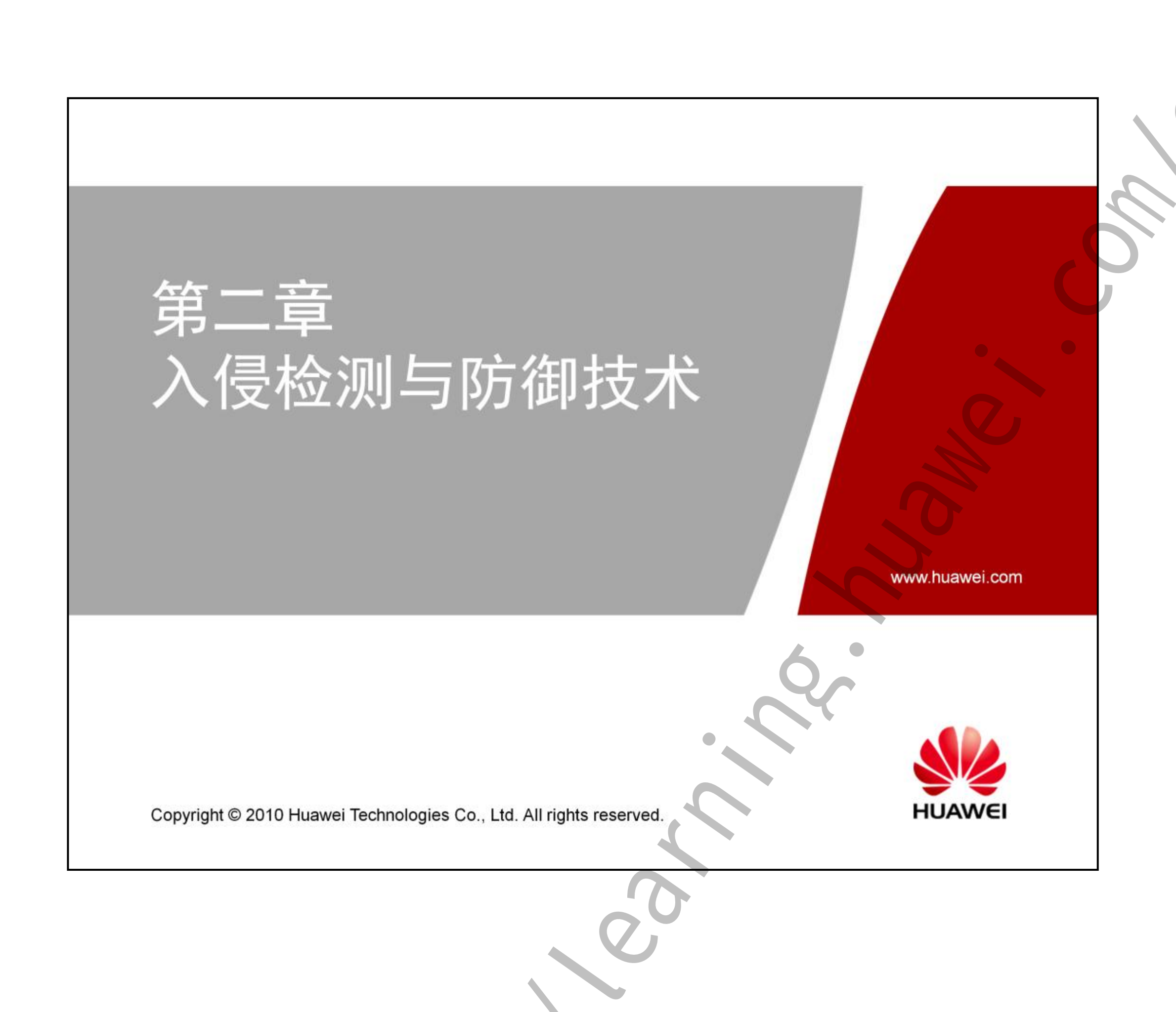
2、下列属于应用层常见的攻击有?

A、缓冲区溢出B、病毒C、CC攻击D、arp欺骗

答案：A|B|C

Thankyou

www.huawei.com


第二章
入侵检测与防御技术
www.huawei.com
HUAWEI



目标

- 学完本课程后，您将能够:
  - 掌握入侵检测与防御技术；
  - 掌握入侵检测技术的应用；
  - 掌握入侵防御技术的应用。



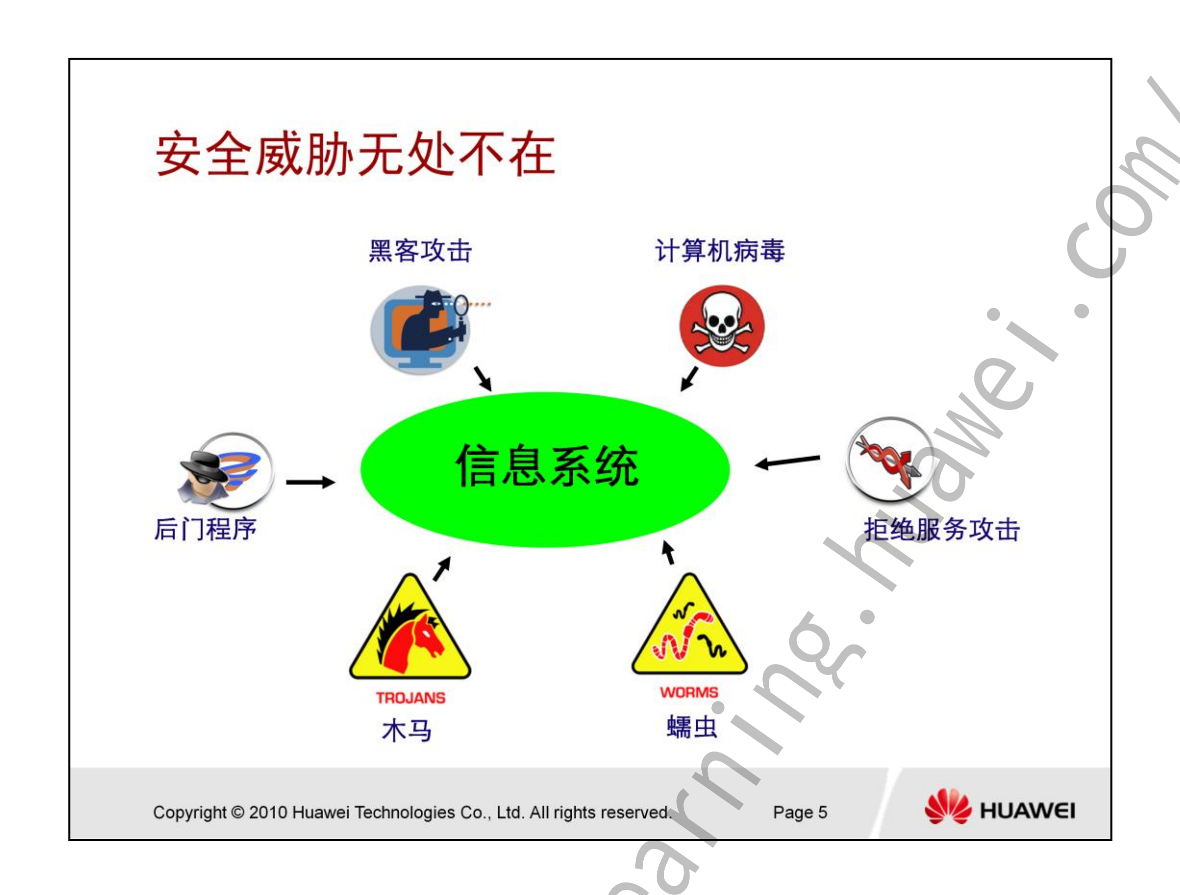


目录





随着信息技术的飞速发展，信息技术给我们的工作、生活带来了更多的便利的同时也改变了我们的生活、工作模式。如今我们可以足不出户，通过电子商务买到自己心仪的商品，通过协同办公解决远在地球另一端的工作问题，通过IM，将自己和朋友的距离拉近。这些都是信息技术发展所带来的好处，但是同时我们也看到了信息技术的发展也带了一些不良的东西，如蠕虫的爆发、垃圾邮件泛滥等不好的东西，这些犹如潘多拉之盒一样。



随着信息时代的来临，信息系统的重要性也凸显出来，电子商务、电子政务、网上办公等，信息系统正在逐渐改变着人们的生活，也标志着信息时代的来临。

在信息时代，由于信息系统固有的缺陷导致信息系统面临各种各样的安全威胁，病毒、蠕虫、各种各样的攻击都对信息系统的完整性、可用性以及机密性产生着威胁。

信息系统面临的挑战

- 网站被黑了，不知道是 谁 什么时候 干的！
- 网站页面访问不了，不知道受到什么样的攻击！
- 信息网络被入侵，调查中缺乏证据！
- 内部数据外泄，不知道谁是内鬼！
- 遭受蠕虫病毒攻击，造成网络瘫痪，但不知道如何 避免和清除这些攻击！
- 无法有效的掌握网络安全状态，无法及时感知安全隐患!



传统的信息安全防御手段（如防火墙）已经无法解决以上这些问题。面对这些挑战我们需要采取新的安全措施与技术。

如何应对？

- 传统的防火墙无法阻止来自应用层的威胁与攻击需要一种全新的技术手段：
  - 具备对常见入侵行为的检测能力，可识别绝大多数的入侵行为，及时感知信息系统所面临的安全隐患；
  - 具备网络监控能力，提供邮件、通讯、文件传输、服务器状态监控，防止信息外泄；
  - 具备丰富的流量统计功能，能够准确掌握网络运行情况和系统安全状态，及时发现网络异常；

答案：入侵检测与防御系统



入侵检测与防御系统能够检测来自应用层的威胁，感知受保护的信息系统所面临的各种安全威胁，记录、监控信息系统中的各项活动。



目录



入侵检测系统的引入

- 入侵

  入侵是指未经授权而尝试访问信息系统资源、窜改信息系统中的数据，使信息系统不可靠或不能使用的行为；入侵企图破坏信息系统的完整性、机密性、可用性以及可控性。

- 典型的入侵行为：
  - 篡改Web网页；
  - 破解系统密码；
  - 复制/查看敏感数据；
  - 使用网络嗅探工具获取用户密码；
  - 访问未经允许的服务器；
  - 其他特殊硬件获得原始网络包；
  - 向主机植入特洛伊木马程序。

问题1：病毒是入侵行为么？

问题2：网络钓鱼是入侵行为么？

 Page 9 

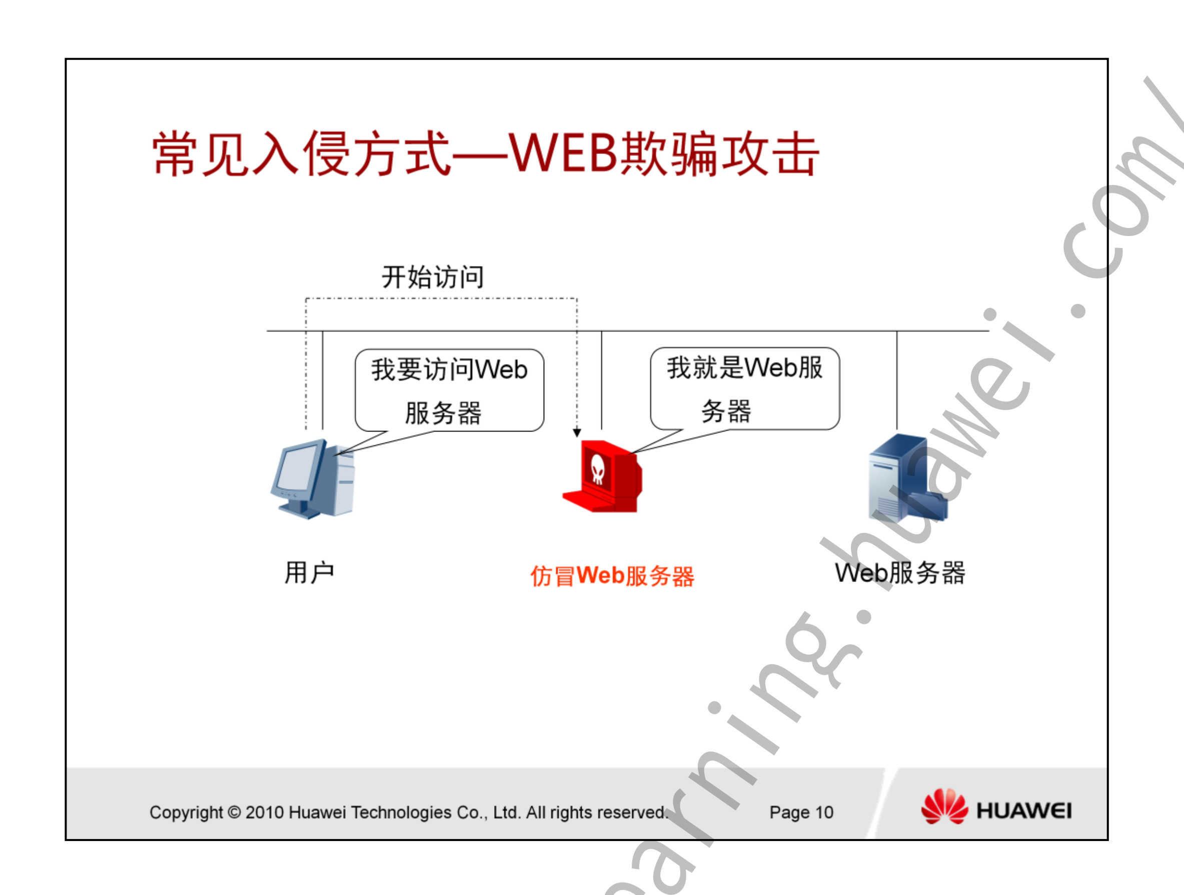
对网页的篡改是目前互联网中经常遇到的问题，篡改网页的动机有得是出于好奇、也有不怀好意的出于政治等因素，甚至有部分是希望通过挂马等手段获取经济利益。

对于在传输中未采取加密手段的网络协议，通过ARP欺骗以及其他手段，可以通过网络嗅探工具轻易地获取协议传输的明文内容，通过简单转换就能获取其中的用户名密码等敏感信息。

什么是网络钓鱼？

网络钓鱼英文叫Phishing，是Fishing和Phone的结合体，这是因为最初的钓鱼作案就是使用的电话，所以使用Ph代替F，创造了“Phishing”这个词。

网络钓鱼利用欺骗性的电子邮件和伪造的Web站点来进行诈骗活动，诈骗者把自己伪装成知名的网站、银行、在线零售商等吸引受害者上当。受害者可能在这些欺骗网站上泄露自己的银行卡账号、密码等敏感信息。



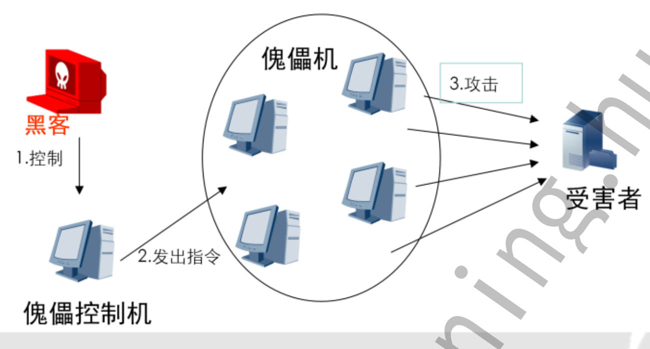
攻击者建立一个人们相信的Web站点的拷贝，然后控制这个Web站点的拷贝，攻击者控制被攻击对象和真的Web服务器之间的所有信息流。攻击者既可以假冒用户给服务器发送数据，也可以假冒服务器给用户发送假冒的信息。

Web欺骗攻击是一种典型的中间人攻击方式。攻击者通过往往通过静态观察，被动获取用户敏感数据或者主动实施破坏，获取用户主机的控制权。Web欺骗攻击往往采取以下两种攻击方式。

- 静态观察
  - 被动地观察整个数据流；
  - 记录浏览者所访问的页面和页面的内容；
  - 记录用户输入的数据和服务器的响应；
  - 大多数在线商务都要填充表格，所以可简单地获得用户的口令；
  - 这种方式比较隐蔽不易被发现。
- 实施破坏
  - 攻击者可以随意修改来往于浏览者和服务器间的信息，比如在网页代码中增加恶意代码，达到入侵用户主机的目的。

常见入侵方式—分布式拒绝服务攻击

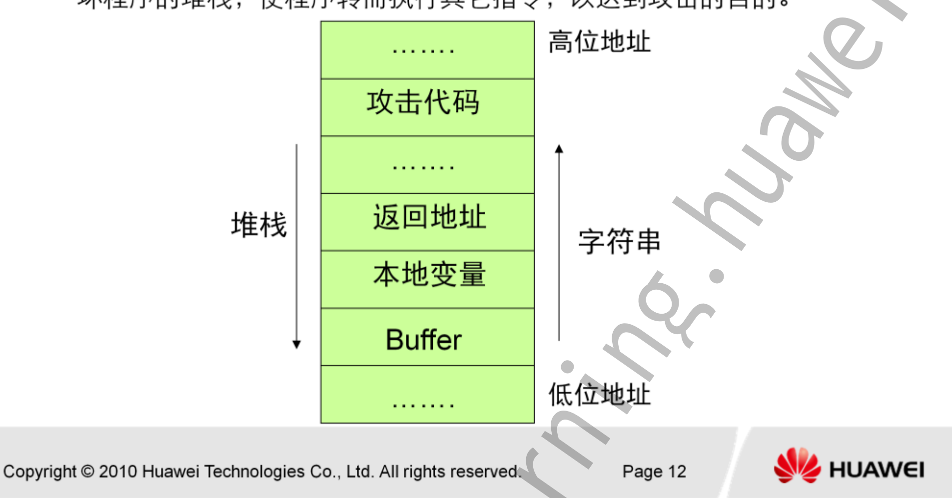
- 拒绝服务攻击
  - 指一个用户占用了大量的共享资源，使系统没有其他的资源给其他合法用户使用的攻击，拒绝服务攻击降低了系统资源的可用性。
  - 系统资源：CPU时间、磁盘空间、网络带宽、打印机、MODEM、甚至是系统管理员的时间等。





最基本的DoS攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。DDoS攻击手段是在传统的DoS攻击基础之上产生的一类攻击方式。单一的DoS攻击一般是采用一对一方式的，当攻击目标CPU速度低、内存或者网络带宽等各项性能指标不高时，它的攻击效果是明显的。

分布式的拒绝服务攻击(DDoS)的原理很简单。DDoS就是利用更多的傀儡机来发起进攻，以比从前更大的规模来进攻受害者。高速广泛连接的网络为DDoS攻击创造了极为有利的条件。如果说DoS是单打独斗，DDoS就是群殴。



缓冲区的溢出原因分析，造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。例如下面程序：

```
void function(char *str) {
char buffer[16];
strcpy(buffer,str)
}
```

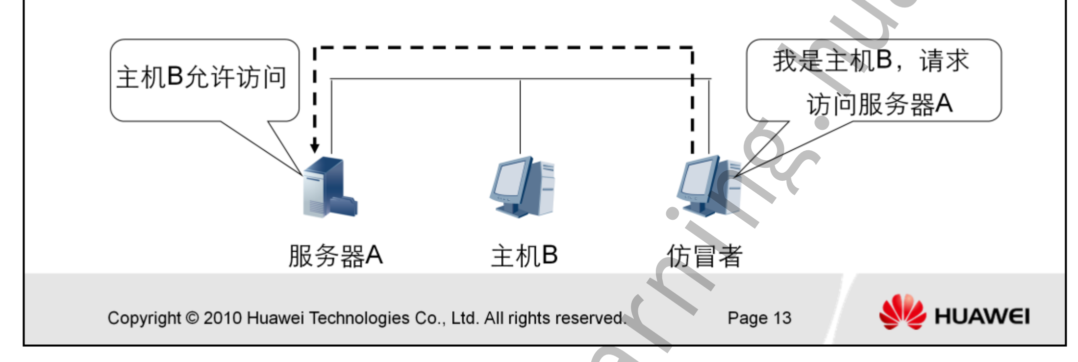
上面的strcpy()将直接把str中的内容copy到buffer中。这样只要str的长度大于16，就会造成buffer的溢出，使程序运行出错。

- 常见的溢出有：
  - 栈溢出；
  - 堆溢出；
  - 整形溢出；
  - 字符串溢出。

早期很多蠕虫都是利用主机的缓冲区溢出漏洞获取主机的控制权，例如：冲击波、震荡波、红色代码等。随着软件开发者对缓冲区溢出问题的认识越来越深刻，这类漏洞也越来越少。

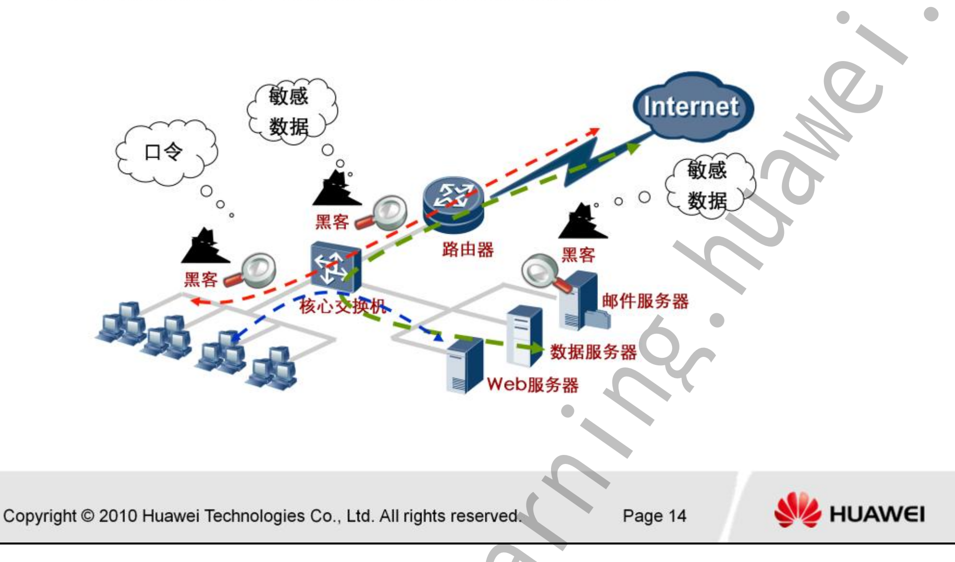
常见入侵方式—IP地址欺骗

- **IP地址欺骗攻击**
  - 伪造某台主机的IP地址，利用主机之间的正常信任关系发动的攻击。
  - 入侵者可以利用IP欺骗的技术获得对主机未授权的访问，因为他可以发出这样的IP包，自称来自内部地址。当目标主机利用基于IP地址的验证来控制对目标系统中的用户访问时，甚至可以获得普通用户或特权的权限。



IP地址和家庭住址一样，如果你要写信给一个人，你就要知道他（她）的地址，这样邮递员才能把信送到，计算机发送信息是就好比是邮递员，它必须知道唯一的“家庭地址”才能不至于把信送错人家。只不过我们的地址使用文字来表示的，计算机的地址用十进制数字表示。

众所周知，在电话通讯中，电话用户是靠电话号码来识别的。同样，在网络中为了区别不同的计算机，也需要给计算机指定一个号码，这个号码就是“IP地址”。每一个IP报文中都是用IP地址作为源和目的地址，通过伪造源地址，攻击者把自己伪装成某台合法的主机，从而达到绕过基于IP地址验证的授权访问体系。在DoS攻击中，攻击者经常使用伪造的源IP地址，达到隐藏自己的目的。



网络侦听，在网络安全上一直是一个比较敏感的话题，作为一种发展比较成熟的技术，侦听在协助网络管理员监测网络传输数据，排除网络故障等方面具有不可替代的作用，因而一直倍受网络管理员的青睐。然而，在另一方面网络侦听也给网络安全带来了极大的隐患，许多的网络入侵往往都伴随着网络侦听行为，从而造成口令失窃，敏感数据被截获等连锁性安全事件。

网络侦听可以在网上的任何一个位置实施，如局域网中的一台主机、网关上或远程网的调制解调器之间等。黑客们用得最多的是截获用户的口令。在网络上，侦听效果最好的地方是在网关、路由器、防火墙一类的设备处，通常由网络管理员来操作。使用最方便的是在一个以太网中的任何一台上网的主机上，这是大多数黑客的做法。

网络侦听需要将主机的网卡设置为混杂模式，工作在混杂模式的网卡，能够接受所有经过网卡的网络报文，哪怕这个报文并不是发给自己的。

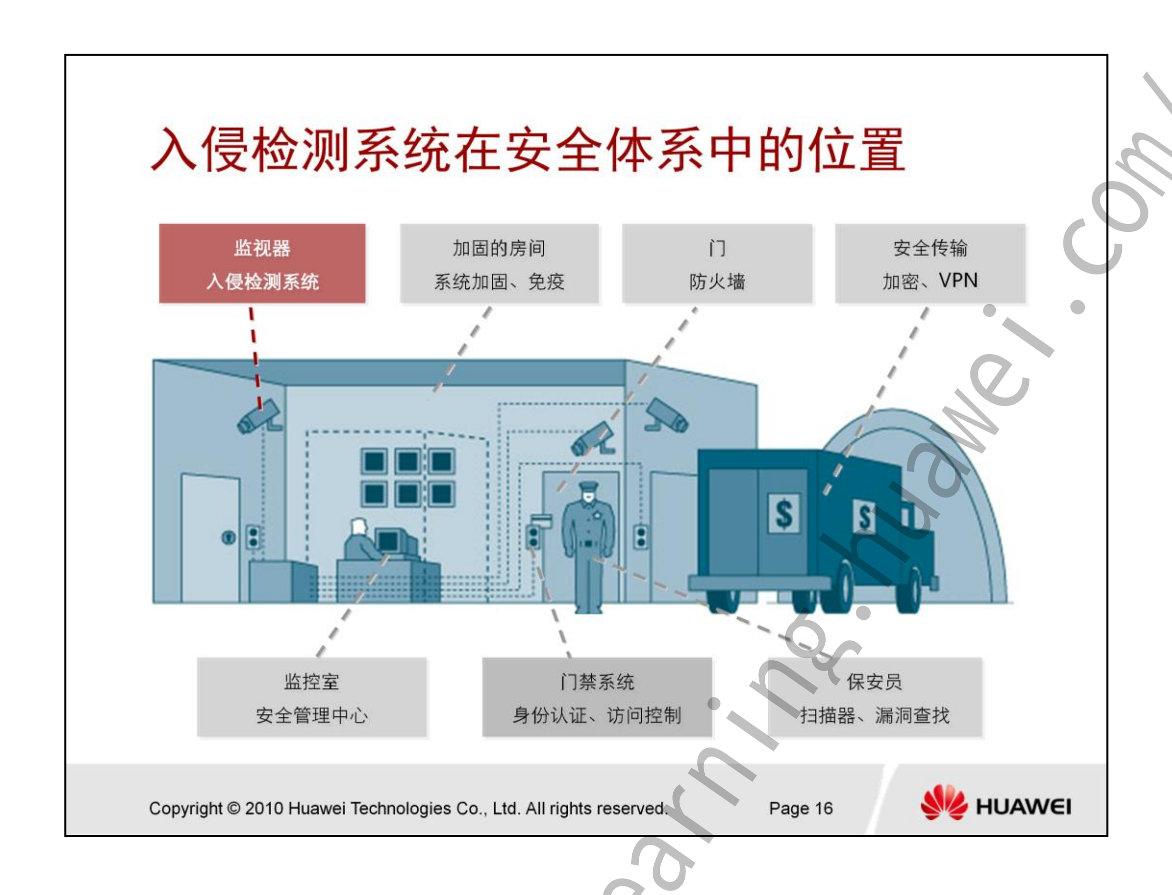
入侵检测

- 入侵检测（ID，Intrusion Detection）
  - 通过监视各种操作，分析、审计各种数据和现象来实时检测入侵行为的过程，它是一种积极的和动态的安全防御技术；
  - 入侵检测的内容涵盖了授权的和非授权的各种入侵行为。
- 入侵检测系统（IDS，Intrusion Detection System）
  - 用于入侵检测的所有软硬件系统；
  - 发现有违反安全策略的行为或系统存在被攻击的痕迹，立即启动有关安全机制进行应对。



入侵检测的内容涵盖了授权的和非授权的各种入侵行为，例如，违反安全策略行为、冒充其他用户、泄露系统资源、恶意行为、非法访问，以及授权者滥用权力等。

入侵检测系统可以通过网络和计算机动态地搜集大量关键信息资料，并能及时分析和判断整个系统环境的目前状态，一旦发现有违反安全策略的行为或系统存在被攻击的痕迹等，立即启动有关安全机制进行应对，例如，通过控制台或电子邮件向网络安全管理员报告案情，立即中止入侵行为、关闭整个系统、断开网络连接等。



在信息安全建设中，入侵检测系统扮演着监视器的角色，通过监控信息系统关键节点的流量，对其进行深入分析，发掘正在发生的安全事件。

一个形象的比喻就是：IDS就像安全监控体系中的摄像头，通过IDS，系统管理员能够捕获关键节点的流量并做智能的分析，从中发现异常、可疑的网络行为，并向管理员报告。

- 防火墙属于串路设备，需要做快速转发，无法做深度检测；
- 防火墙无法正确分析掺杂在允许应用数据流中的恶意代码 ，无法检测来自内部人员地恶意操作或误操作；
- 防火墙属于粗粒度的访问控制，IDS属于细粒度的检测设备，通过IDS可以更精确地监控现网；
- IDS可与防火墙、交换机进行联动，成为防火墙的得力“助手”，更好、更精确的控制外域间地访问；
- IDS可灵活、及时的进行升级，策略地配置操作方便灵活。

入侵检测系统的分类

- 基于主机的入侵检测系统（HIDS）
  - 主要用于保护运行关键应用的服务器；
  - 通过监视和分析主机的审计记录和日志文件来检测入侵；
  - 可监测系统、事件、Win NT下的安全记录以及Unix环境下的系统记录，从中发现可疑行为；
  - 侦听主机的端口的活动，并在特定端口被访问时向管理员报警；
- 基于网络的入侵检测系统（NIDS）
  - 主要用于实时监控网络关键路径的信息，侦听网络上的所有分组，采集数据，分析可疑对象；
  - 使用原始网络包作为数据源；
  - 通过网络适配器来实时监视，并分析通过网络的所有通信业务，也可能采用其他特殊硬件获得原始网络包；
  - 提供了许多基于主机的入侵检测系统无法提供的功能；



根据入侵检测系统部署的位置的不同，往往将其分为HIDS和NIDS，基于主机的入侵检测系统部署在主机上，通过检视主机的安全。HIDS部署简单，适合加密的环境，但HIDS需要依赖主机的OS，如果信息系统中主机数量繁多，部署与管理将比较麻烦；NIDS部署在信息网络的关键节点处，监视网络流量，属于独立性部署，对信息系统的主机没有任何影响，缺陷就是对加密的流量无法进行检视与处理。

基于主机的入侵检测系统（HIDS）

- 优点
  - 能确定攻击是否成功
  - 监控粒度更细
  - 配置灵活
  - 可用于加密的以及交换的环境
  - 对网络流量不敏感
  - 不需要额外的硬件；
- 缺点
  - 占用主机的资源，在服务器上产生额外的负载；
  - 缺乏平台支持，可移植性差，应用范围受到严重的限制







- 优点
  - 能确定攻击是否成功，攻击目的即为主机，可根据已发生的事件信息更准确地判断攻击是否成功；
  - 监控粒度更细，监控的目标明确、视野集中；
  - 可检测一些基于网络的IDS不能检测的文件；可以容易的监控系统的一些活动，如对敏感文件、目录、程序或端口的存取，还可监视通常只有管理员才能实施的非正常行为。系统的一些活动，有时并不通过网络传输，即使通过网络传输，也不能提供足够多的信息；
  - 配置灵活；
  - 可用于加密的以及交换的环境；
  - 对网络流量不敏感；
  - 不需要额外的硬件。
- 缺点
  - 占用主机的资源，在服务器上产生额外的负载；
  - 缺乏平台支持，可移植性差，应用范围受到严重的限制。

基于网络的入侵检测系统（NIDS）

- 优点
  - 监测速度快
  - 隐蔽性好
  - 视野更宽
  - 较少的监测器
  - 攻击者不易转移证据
  - 操作系统无关性
  - 不占用被保护的设备上的资源
- 缺点
  - 只监视本网段活动，精确度不高
  - 在交换环境下难以配置
  - 防入侵欺骗的能力较差
  - 难以定位入侵者

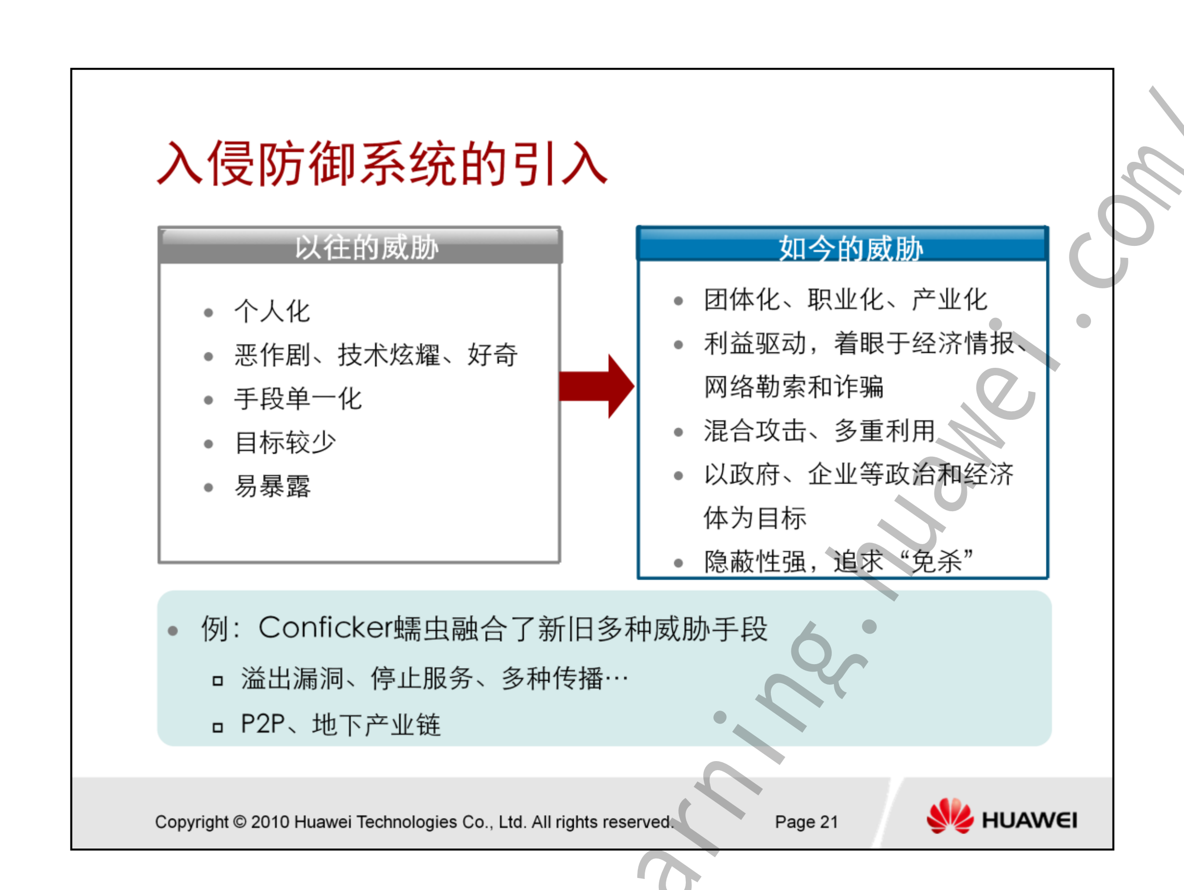
外部网 DMZ 内部网
ERP 文件共享 WebE-mail
Internet
交换机
流量镜像
NIP
NIP引擎 NIP控制台
入侵检测 WEB监控 邮件监控 MSN监控 文件传输监控 会话监控 服务器监控

- 监测速度快，能在微秒或秒级发现问题，基于主机的IDS要依靠对最近几分钟内的审计记录的分析；
- 隐蔽性好，基于网络的监视器不运行其他的应用程序，不提供网络服务，可以不响应其他计算机，因此不易受到攻击；
- 视野更宽，可检测主机无法检测到的攻击；
- 较少的监测器，一个监测器可保护一个共享的网段，不需要很多监测器；
- 攻击者不易转移证据，使用正在发生的网络通信进行对实时攻击的检测，所以攻击者无法转移证据，被捕获的数据不仅包括攻击的方法，还包括可以识别黑客身份和对其进行起诉的信息；
- 操作系统无关性，可以配置在专门的机器上，不会占用被保护的设备上的任何资源；
- 入侵检测只能检测到源地址和目的地址，不能识别地址是否违造，所以难以定位真正的入侵者。



目录





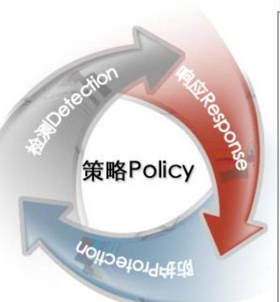
随着信息系统的发展，以及信息系统面临的威胁的变化，主要是威胁越来越多以及手段更加隐蔽，变化很多，往往都是基于利益驱动。

IDS缺少主动防御的能力的弊端也越来越明显，信息系统需要能够主动应对威胁的安全系统，这样IPS就问世了。IPS结合了IDS对入侵行为检测的能力并能够迅速截断已有的攻击行为，减少信息系统面临威胁的损失。

事件监控IDS→IPS

入侵检测IDS

- 提供安全威胁监控平台
- 具备分析、审计系统
- 强化风险管理能力
- 及时了解网络安全状况
- 为网络安全风险控制提供依据



入侵防御IPS

- 提供安全威胁监控及实时 响应、控制能力
- 具备分析、审计及接入控 制系统
- 强化风险控制能力，降低安全影响
- 优化风险控制环境



P2DR是一种动态的网络安全模型，包含有Protection（防护）、Detection（检测）、Response（响应）、Policy（策略）四个部分组成。由Detection（检测）、Response（响应）、Protection（防护）组成一个动态的环，围绕安全策略而展开。

P2DR的核心思想是：以Policy安全策略为核心，通过各种入侵检查等手段进行安全漏洞检测。入侵检测使对信息系统的防护由静态转化为动态，为系统安全事件提供快速响应（Response）。当发现信息系统有安全异常时，根据制定好的信息系统安全策略快速做出反应，从而达到保护系统安全的目的。

入侵防御系统

- 入侵防御系统（IPS，Intrusion Prevention System）
  - 定义：在发现入侵行为时能实时阻断的入侵检测系统。
  - IPS使得IDS和防火墙走向统一
  - IPS在网络中一般有两种部署方式:。

旁路

SPAN:接在交换机上，通过交换机做端口镜像。

TAP:通过专用的流量镜像设备，部署在网络边界。

直路

Inline:串接在网络边界，在线部署，在线阻断。



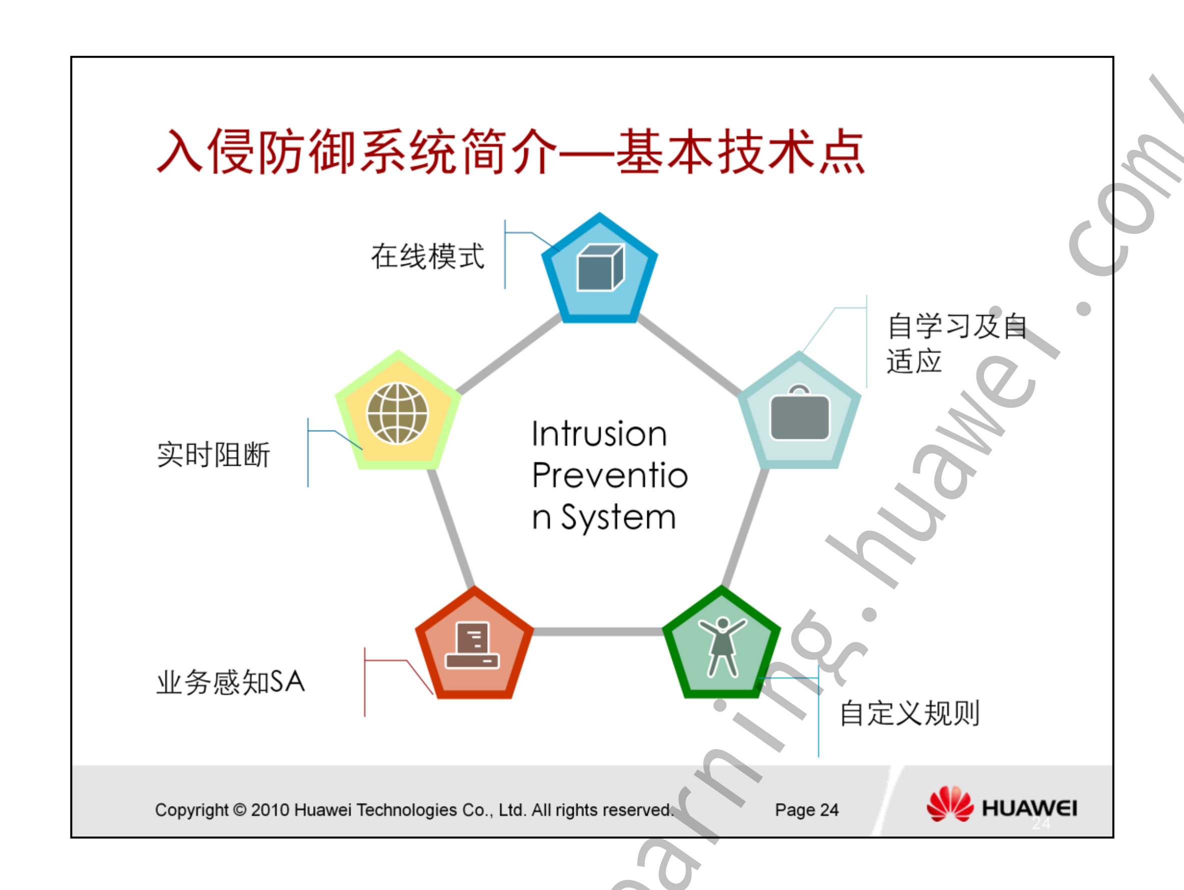
入侵防御系统（IPS，Intrusion Prevention System），在发现入侵行为时能实时阻断的入侵检测系统。

IPS是一种智能化的入侵检测和防御产品，它不但能检测入侵的发生，而且能通过一定的响应方式，实时地中止入侵行为的发生和发展，实时地保护信息系统不受实质性的攻击。

SPAN也叫做端口镜像或者端口监控，是通过交换机配置将某个端口或某组端口的流量复制到另外的端口实现的。

TAP是Test Access Point的首字母缩写，粗浅的说，Tap的概念类似于“三通”的意思，即原来的流量正常通行，同时分一股出来供监测设备分析使用。对Tap这个词的翻译，比较通用就是分光器/分路器。分光是数据通过光纤传输；分路是数据通过网线传输。其实这只是最简单的Tap的概念，目前的技术发展已经产生出很多种的Tap：有可以把多条链路汇聚起来的Tap、有把一条链路流量分成几份的Tap、有过滤Tap、有Tap switch等等，已经不能再用“三通”这个词去简单概括了。Tap的出现是整个监控/监测领域的巨大革命，它从根本上改变了监测分析系统的接入方式，使得整个监测系统有了完整灵活的解决方案。

- Span：接在交换机旁边，作为端口映像；
- Tap：接在交换机与路由器中间，旁路安装，拷贝一份数据到IPS中；
- Inline：接在交换机与路由器中间，在线安装，在线阻断攻击。



入侵保护系统的两大基本技术点：SA与在线模式。

- 在线模式（Inline）：能够让IPS实时阻断到发现的网络攻击行为，避免IDS发现攻击，而无法实时阻止攻击行为发生的缺陷，最大限度的提升系统的安全性；
- 自学习与自适应：IPS能够通过自学习与自适应将系统的漏报与误报降低到最低，减少对业务的影响；
- 自定义规则：IPS能够自定义入侵防御规则，最大限度的对最新的威胁作出反应；
- 业务感知：让IPS能够检测到基于应用层的异常与攻击；
- 实施阻断：IPS因为采取的是在线部署方式，所以能够在发现攻击的同时实时阻断攻击，最大限度的提高了保护对象的安全性。



目录



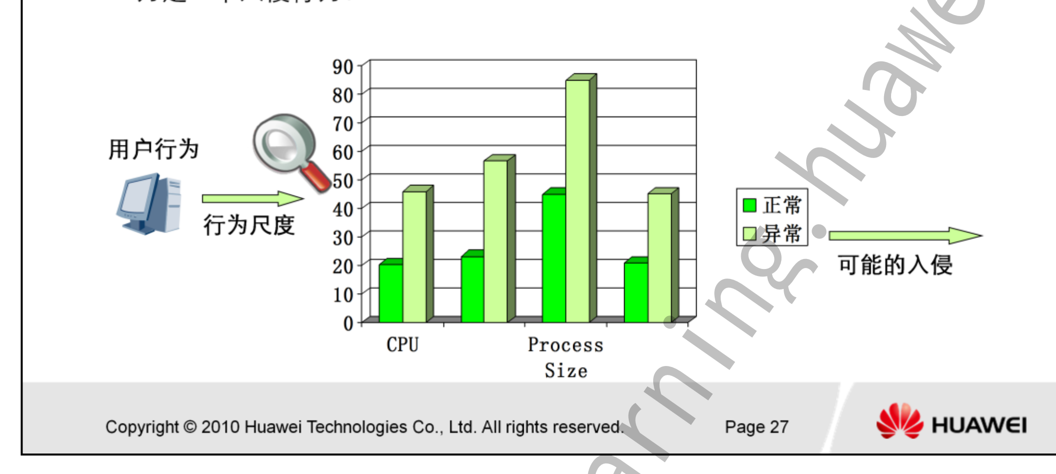
入侵检测技术

- 异常检测模型（Anomaly Detection）
  - 首先总结正常操作应该具有的特征（用户轮廓），当用户活动与正常行为有重大偏离时即被认为是入侵
- 误用检测模型（Misuse Detection）
  - 收集非正常操作的行为特征，建立相关的特征库，当检测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵

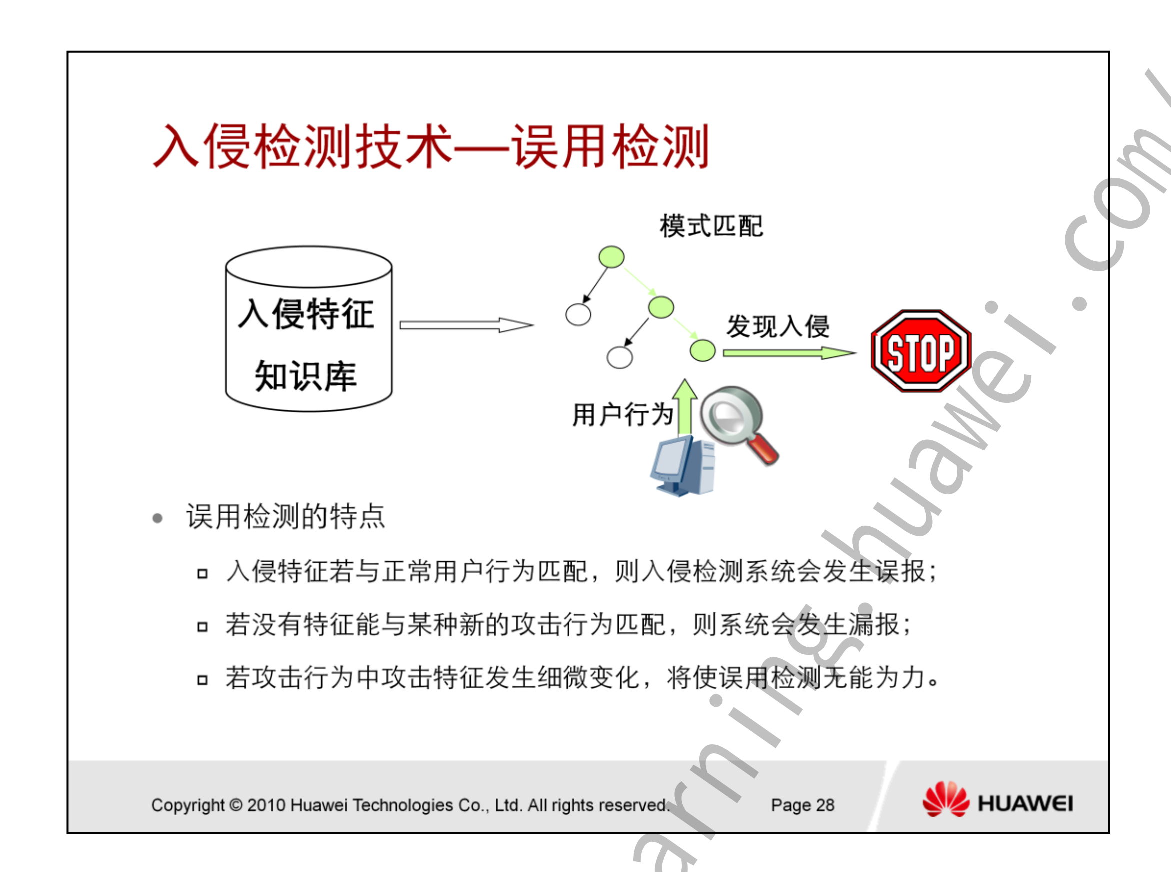


通过对系统审计数据的分析建立起系统主体(单个用户、一组用户、主机，甚至是系统中的某个关键的程序和文件等)的正常行为特征轮廓；检测时，如果系统中的审计数据与已建立的主体的正常行为特征有较大出入就认为是一个入侵行为。

一般采用统计或基于规则描述的方法建立系统主体的行为特征轮廓，即统计性特征轮廓和基于规则描述的特征轮廓。



一般采用统计或基于规则描述的方法建立系统主体的行为特征轮廓，即统计性特征轮廓和基于规则描述的特征轮廓。



通过检测用户行为中的那些与某些已知的入侵行为模式类似的行为或那些利用系统中缺陷或是间接地违背系统安全规则的行为，来检测系统中的入侵活动，是一种基于已有的知识的检测。

这种入侵检测技术的主要局限在于它只是根据已知的入侵序列和系统缺陷的模式来检测系统中的可疑行为，而不能处理对新的入侵攻击行为以及未知的、潜在的系统缺陷的检测。

异常检测与误用检测的优缺点对比

异常检测

- 优点：
  - 不需要专门的操作系统缺陷特征库；
  - 有效检测对合法用户的冒充检测。
- 缺点：
  - 建立正常的行为轮廓和确定异常行为轮廓的阀值困难。
  - 不是所有的入侵行为都会产生明显的异常。



误用检测

- 优点：
  - 可检测所有已知入侵行为。
  - 能够明确入侵行为并提示防范方法。
- 缺点：
  - 缺乏对未知入侵行为的检测。
  - 对内部人员的越权行为无法进行检测。

入侵检测系统的两个重要指标

- 漏报(false negative)
  - 指攻击事件未被入侵检测系统检测出来
- 误报(false positive)
  - 入侵检测系统把正常事件识别为攻击并报警
  - 误报率与检出率(Detection Rate)成正比例关系

讨论：漏报和误报哪个更糟糕?

漏报和误报哪个更糟糕，需要结合业务环境（是业务优先还是安全优先）。



目录



入侵防御系统原理

- IPS检测深度
  - IPS拥有数目众多的过滤器，能够防止各种攻击；
  - 数据包处理引擎是专业化定制的集成电路， 可以深层检查数据包的内容。
- IPS特征匹配
  - 依据数据包中的报头信息对流经IPS的数据包都被分类；
  - 每种过滤器设有相应的过滤规则，负责分析相对应的数据包。



- IPS检测深度

IPS实现实时检查和阻止入侵的原理在于IPS拥有数目众多的过滤器，能够防止各种攻击。当新的攻击手段被发现之后，IPS就会创建一个新的过滤器。IPS数据包处理引擎是专业化定制的集成电路，可以深层检查数据包的内容。如果有攻击者利用Layer 2 （介质访问控制）至Layer 7（应用）的漏洞发起攻击，IPS能够从数据流中检查出这些攻击并加以阻止。传统的防火墙只能对Layer 3或Layer 4进行检查，不能检测应用层的内容。防火墙的包过滤技术不会针对每一字节进行检查，因而也就无法发现攻击活动，而IPS可以做到逐一字节地检查数据包。

- IPS特征匹配

所有流经IPS的数据包都被分类，分类的依据是数据包中的报头信息，如源IP地址和目的IP地址、端口号和应用域。每种过滤器负责分析相对应的数据包。通过检查的数据包可以继续前进，包含恶意内容的数据包就会被丢弃，被怀疑的数据包需要接受进一步的检查。

针对不同的攻击行为，IPS需要不同的过滤器，每种过滤器都设有相应的过滤规则。

IPS技术

- IPS协议识别
  - 协议分析与跟踪是IPS设备的关键点；
  - IPS不但要分析和跟踪网络层、传输层的协议，还要对众多的应用层协议进行分析、跟踪。
- 深度检测和入侵抵御
  - 根据预先设定的安全策略，对流经的每个报文进行深度检测；
  - 一旦发现隐藏于其中网络攻击，可以根据该攻击的威胁级别立即采取抵御措施 。



- IPS协议识别

通过前面的分析，我们可以看到协议分析与跟踪对IPS设备的重要性。与传统防火墙不同的是，IPS不但要分析和跟踪IP、ICMP、UDP、TCP这几种网络层、传输层的协议，而且，还要对HTTP、HTTPS、FTP、TFTP、SNMP、Telnet、SMTP、POP、DNS、RPC、LDAP、ICQ、MSN、Yahoo Messenger等众多的应用层协议进行分析、跟踪。

- 深度检测和入侵抵御

对于部署在数据转发路径上的IPS，可以根据预先设定的安全策略，对流经的每个报文进行深度检测（协议分析跟踪、特征匹配、流量统计分析等），如果一旦发现隐藏于其中网络攻击，可以根据该攻击的威胁级别立即采取抵御措施，这些措施包括（按照处理力度）：向管理中心告警；丢弃该报文；切断此次应用会话；切断此次TCP连接。

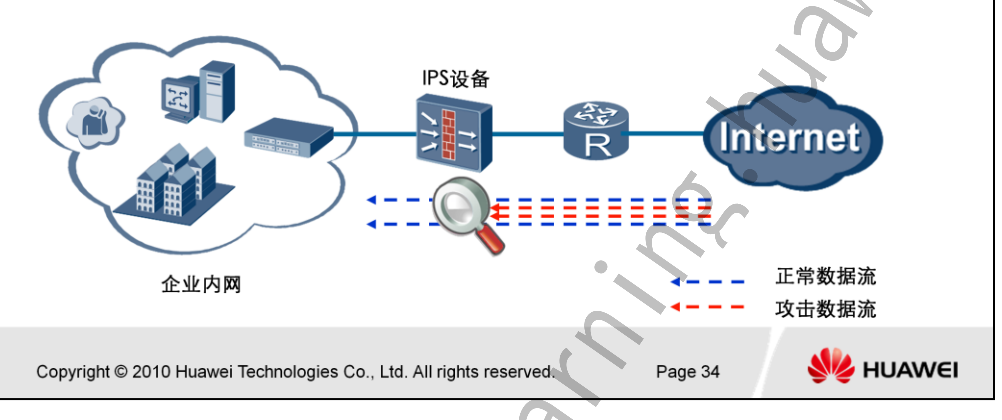
- 总结

随着系统漏洞不断被发现，企业网络面临的安全威胁越来越复杂了。尽管这些攻击可以绕过传统的防火墙，设置在网络周边或内部网络中的入侵防御系统（IPS）仍然能够有效阻止这些攻击，为那些未添加补丁或配置不当的服务器提供保护。

入侵检测系统(IDS)可以监视网络传输并发出警报，但并不能拦截攻击。而IPS则能够对所有数据包仔细检查，立即确定是否许可或禁止访问。 当新的弱点被发现之后，IPS就会创建一些新的规则库，试探攻击这些弱点的任何恶意企图都会立即受到拦截。

IPS部署点

IPS是通过直接嵌入到网络流量中实现这一功能的，即通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中。这样一来，有问题的数据包，以及所有来自同一数据流的后续数据包，都能在IPS设备中被清除掉。

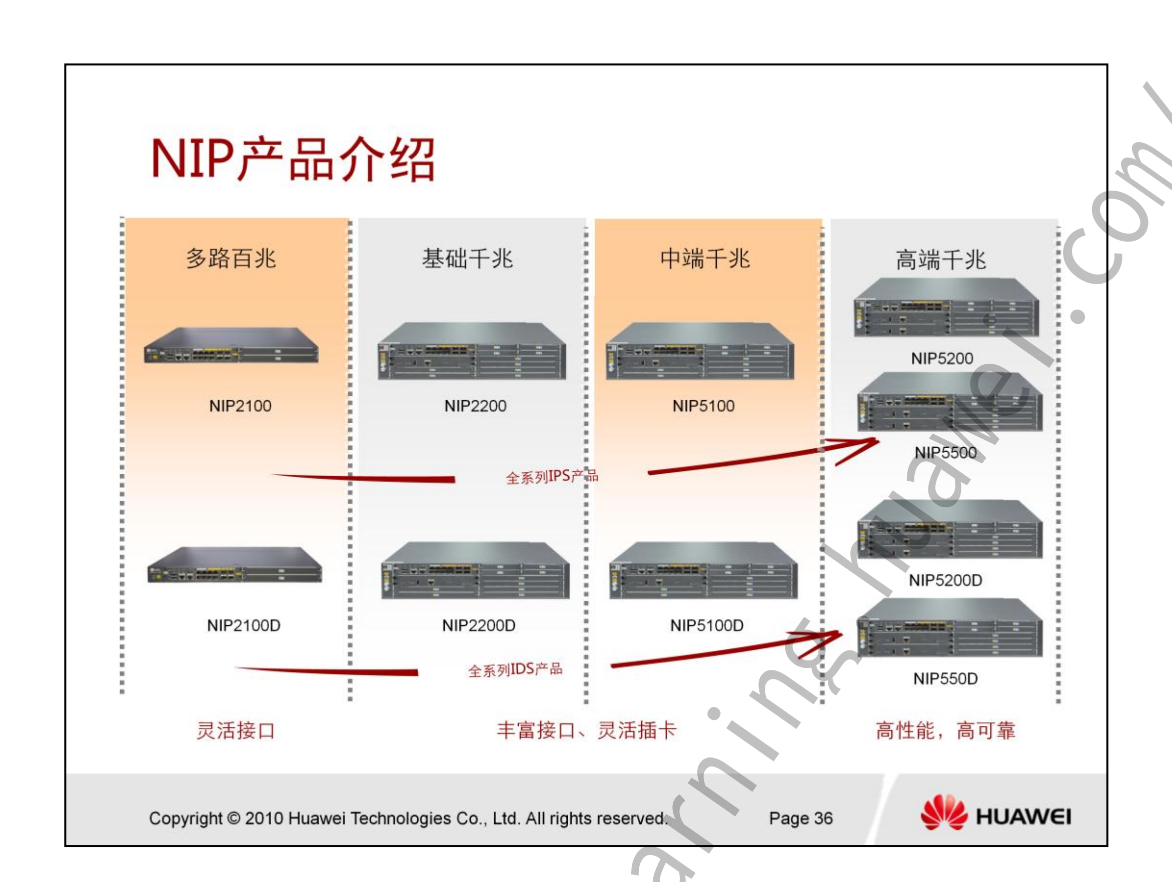


HUAWEI



目录





NIP产品介绍
多路百兆
基础千兆
中端千兆
高端千兆
NIP2100
NIP2200
NIP5100
NIP5200
NIP5500
全系列IPS产品
NIP2100D
NIP2200D
NIP5100D
NIP5200D
NIP550D
全系列IDS产品
灵活接口
丰富接口、灵活插卡
高性能，高可靠
Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.
Page 36
HUAWEI

NIP Manager

NIP Manager集中管理



实时报表 分析



- 基于Web的单机配置和NIP Manager集中管理方式；
- 智能化报表、日志功能，全面展示网络实时状况、历史信息及攻击排名、流量趋势走向；
- 定时网络健康状态报告，指导网络加固及 IT 活动实施；







目录



华为 NIP 领先的硬件架构

多核处理器

- 实现对网络报文的通用预处理；协议智能识别；DDoS攻击防护

FPGA 转发加速

- 实现对安全流量的快速转发

ESP 应用层加速

- 实现对应用层威胁的加速检测及响应处理

8 核网络报文处理器，实现会话的快速连接及网络报文预处理

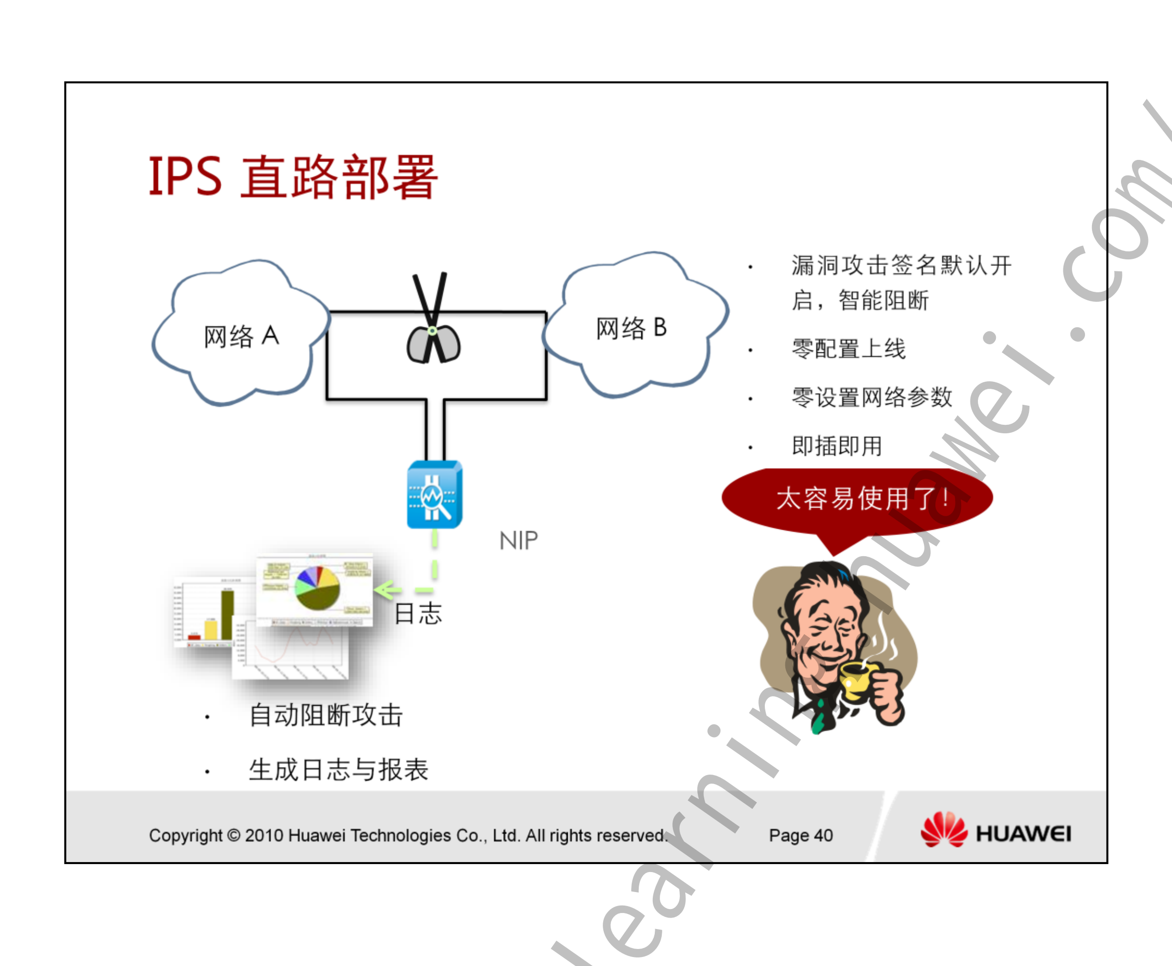
ESP加速板卡实现应用层报文的灵活，快速处理

FPGA卡实现报文的快速转发，最大限度的降低网络时延

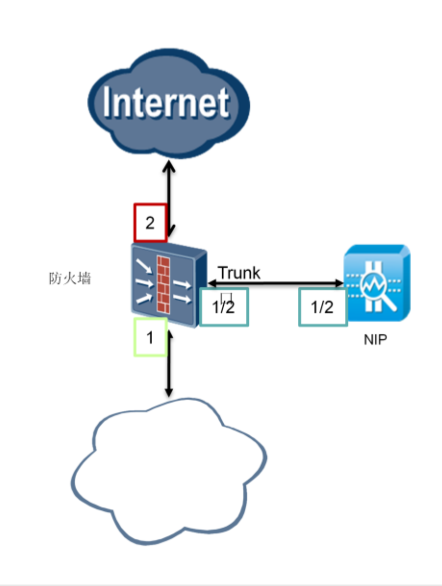


Page 39

HUAWEI


IPS 直路部署
网络 A
网络 B
NIP
日志
漏洞攻击签名默认开启，智能阻断
零配置上线
零设置网络参数
即插即用
太容易使用了！
自动阻断攻击
生成日志与报表
Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.
Page 40
HUAWEI

IPS 旁挂部署



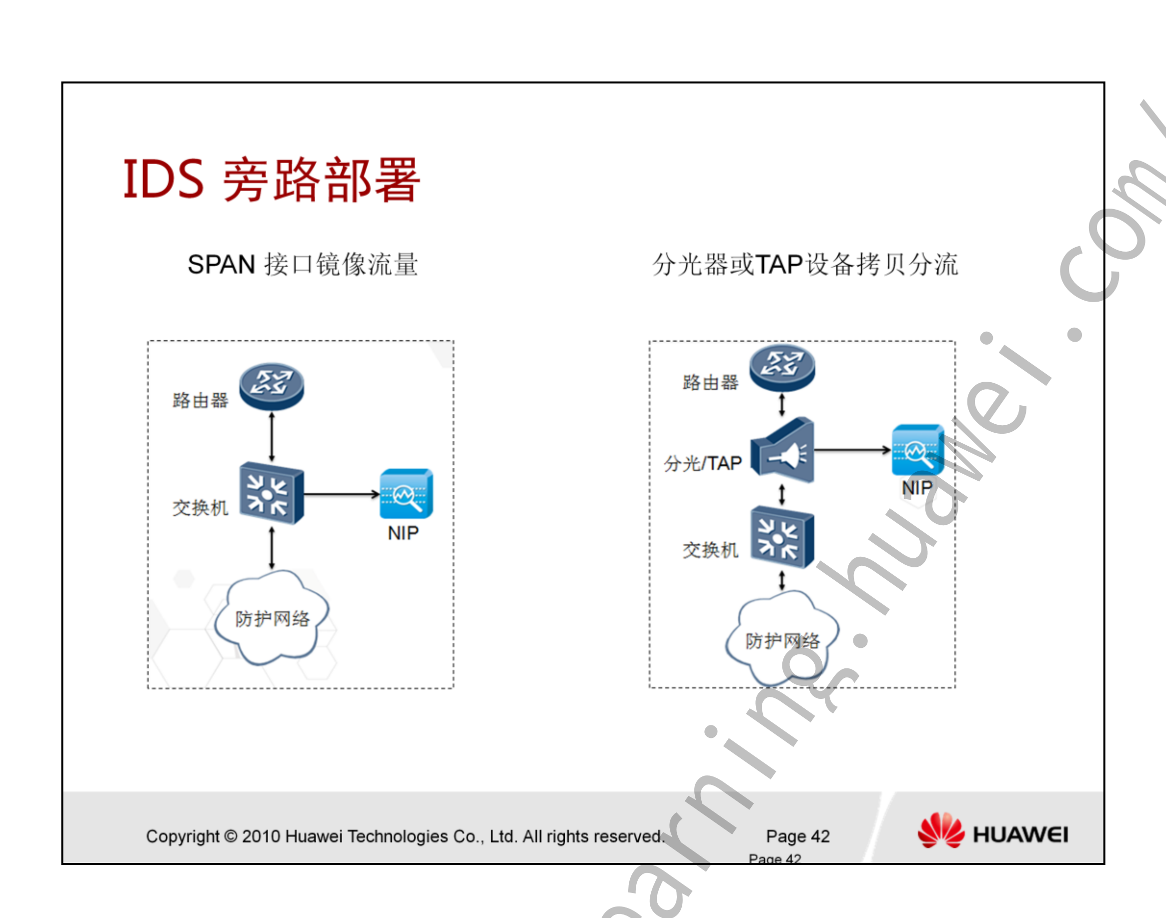


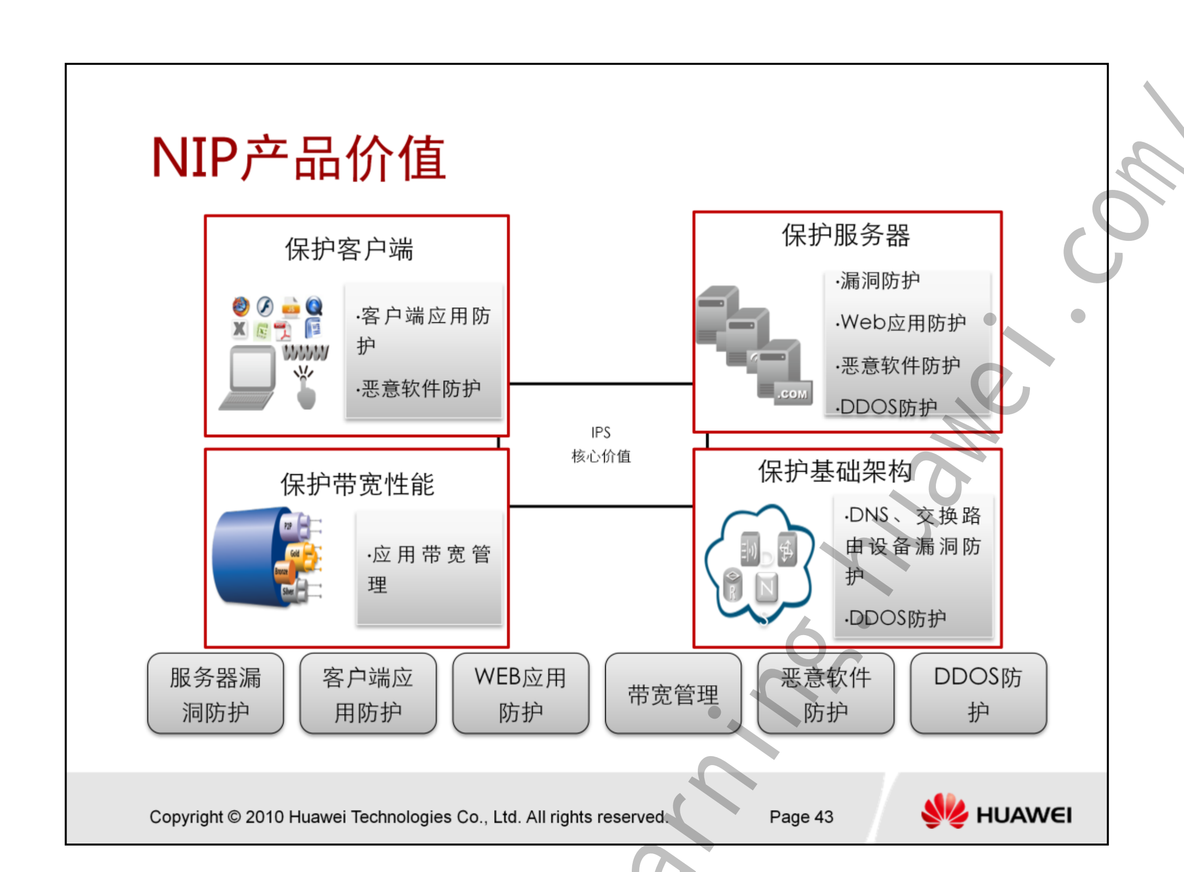
VLAN 旁挂组网

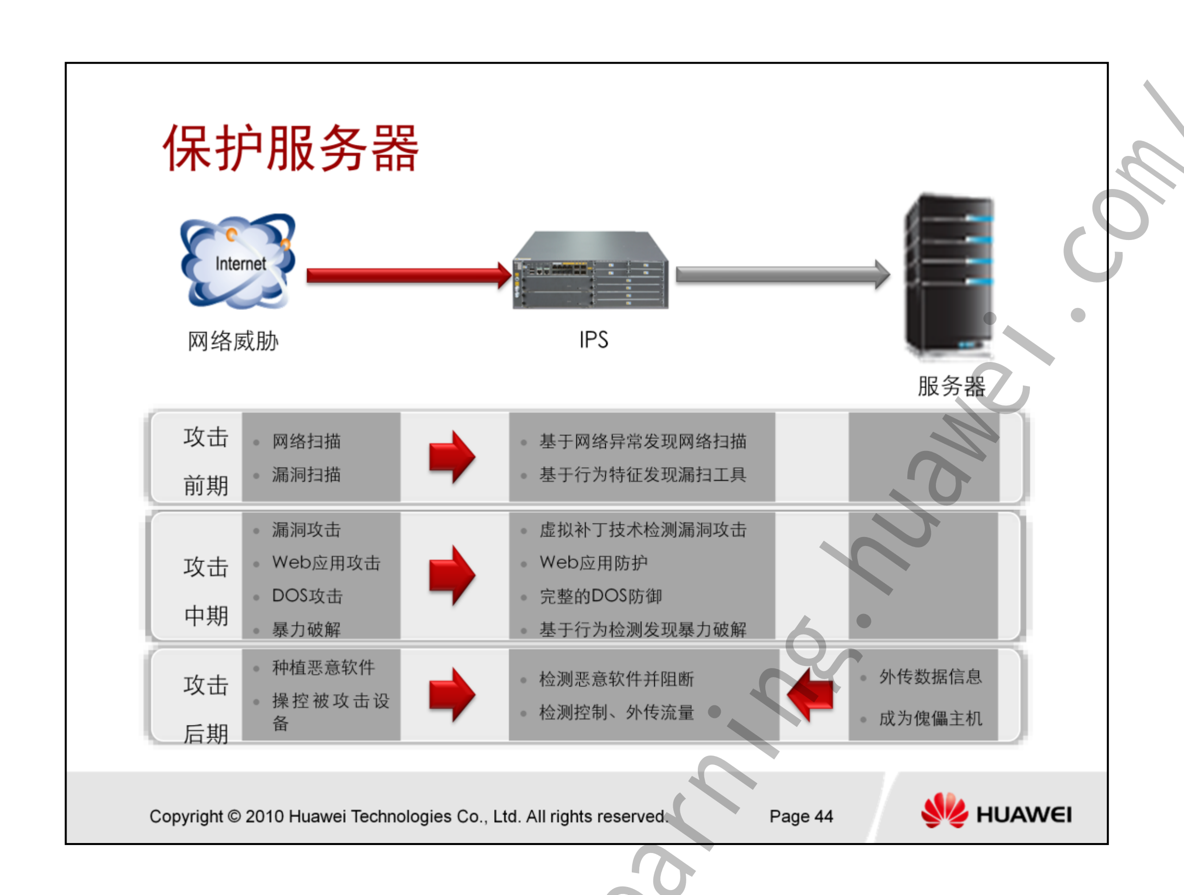
- 防火墙设置两个VLAN， VLAN1 和VLAN2
- NIP 上通过一个物理接口，设置VLAN转换对：VLAN1 与 VLAN2 标签互换
- 通过防火墙VLAN 1接口上行的流量会由右侧Trunk口发给NIP，NIP完成入侵检测后把VLAN1的标签换成VLAN2标签返回给防火墙，再发到Internet。
- Internet 返回的流量路则路径相反
- NIP 支持基于VLAN配置安全策略及记录日志信息

Page 41

HUAWEI


IDS 旁路部署
SPAN 接口镜像流量
分光器或TAP设备拷贝分流
路由器
交换机
NIP
防护网络
路由器
分光/TAP
NIP
交换机
防护网络
Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.
Page 42
HUAWEI

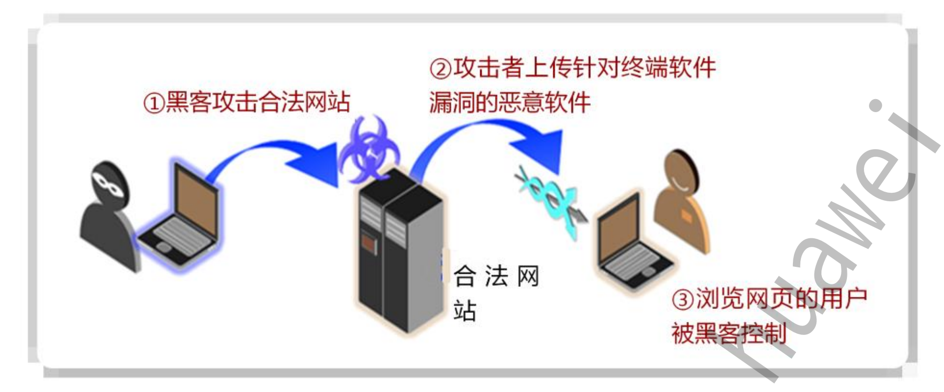

NIP产品价值
保护客户端
·客户端应用防护
·恶意软件防护
保护服务器
·漏洞防护
·Web应用防护
·恶意软件防护
·DDOS防护
IPS
核心价值
保护带宽性能
·应用带宽管理
保护基础架构
·DNS、交换路由设备漏洞防护
·DDOS防护
服务器漏洞防护
客户端应用防护
WEB应用防护
带宽管理
恶意软件防护
DDOS防护
Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.
Page 43
HUAWEI



针对服务器攻击的整个过程均提供完善的防护措施：前期、中期、后期



保护客户端



- 浏览器及其插件（Java、ActiveX等）的安全防护；
- PDF、Word、Flash、AVI等文件层的攻击防护；
- 木马、蠕虫及对操作系统的攻击防护；
- URL 关键字过滤



讲解客户端攻击的整个过程，及IPS在其中发挥的作用





- 基于虚拟补丁技术，对基础网络设备的漏洞进行防护；
- 综合7种流量检测技术，对各种网络DOS、应用DOS（针对DNS、HTTP、SIP的基础服务）提供整体防护；
- 提供流量自学习功能，保障对各种异常流量攻击的准确检测；



将两个方面：设备系统漏洞的防护，对设备的DOS攻击防护

保护带宽性能



- 有效保障业务带宽，提高企业IT治理水平：
- 对P2P、流媒体等应用带宽控制，保障网络资源有效使用；
- 限制使用IM、游戏、股票等应用，保障工作效率；
- Web Mail、在线存储以及隧道传输等控制，防止机构内部文件非法外传；
- 基于IP地址的限流



威胁防护全面

服务器攻击检测	客户端攻击检测	Web攻击检测
• 防止对HTTP、FTP、DNS、Mail等服务器的各种攻击：缓冲去溢出、系统或服务漏洞攻击、暴力破解等 • 文件型病毒扫描检测	• 针对客户日常应用，如：Office文档、PDF,多媒体以及浏览器提供深度检测，避免客户端免成为Botnet或网马的受害者 • 文件型病毒扫描检测	• 检测Web应用相关攻击，包括Web2.0及后台数据库；对注入攻击、跨站脚本、目录穿越等提供重点防护

网络滥用检测	恶意软件检测	DDOS检测
• 检测P2P、视频应用，保障业务带宽 • IM、在线存储、web邮箱、网络隧道证券及游戏的访问，影响员工效率 • 基于 IP 地址带宽限流	• 蠕虫、木马、间谍软件 • 僵尸网络 • 广告软件等 • 文件型病毒扫描检测	• 针对网络流量的DoS • 针对应用服务的DoS • 针对操作系统的DoS • 扫描探测



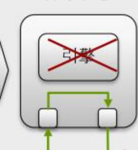
可靠性

电信级硬件设计

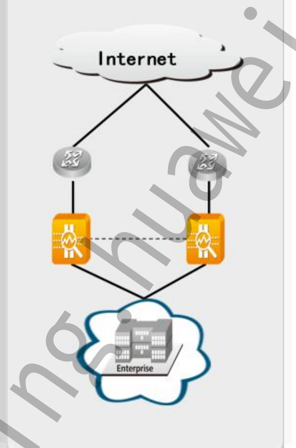
- 支持温度监控、风扇热插拔，可适应恶劣环境应用
- 双电源互相热备份，并且支持热插拔
- 按照电信产品要求设计

设备自身失效保护

- 基于软件的Bypass
- 基于硬件的Bypass
  - 电口Bypass
  - 多模光口Bypass
  - 单模光口Bypass



HA高可靠部署

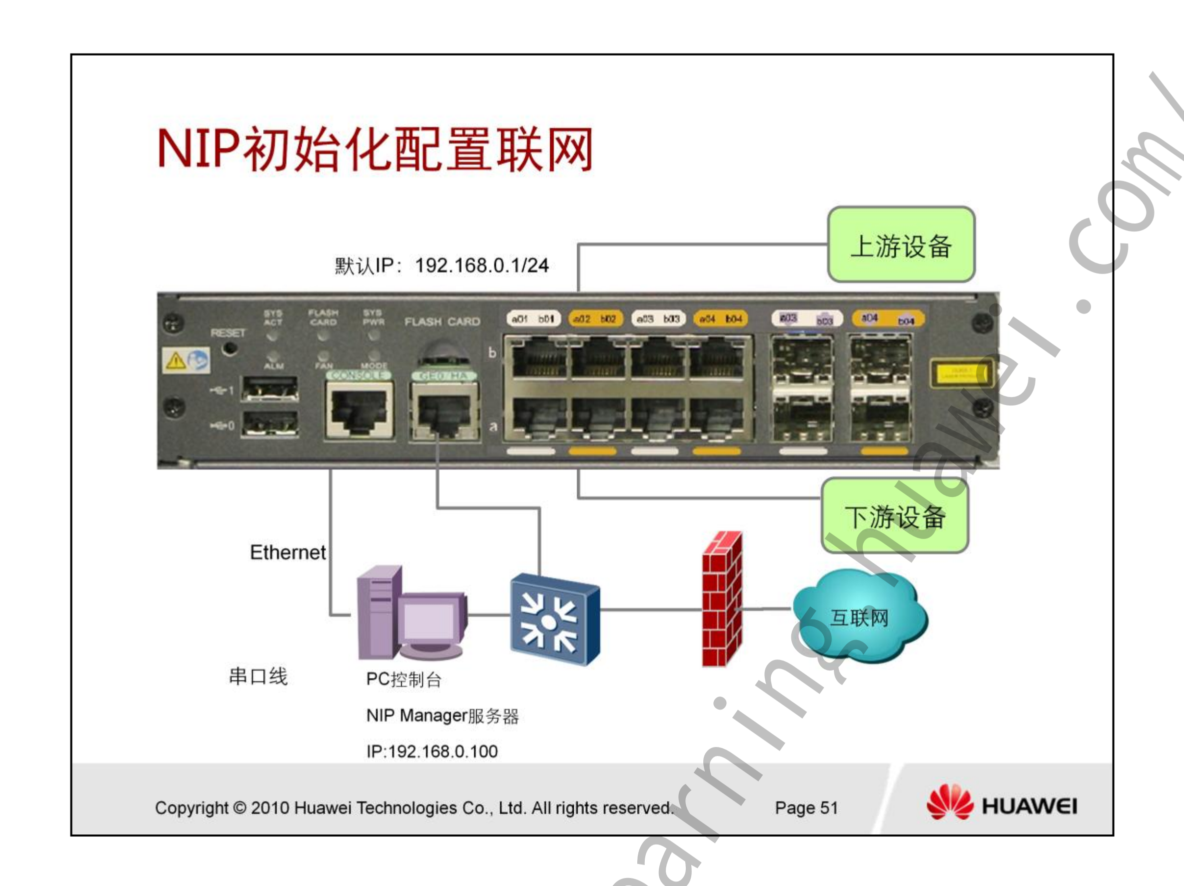






目录

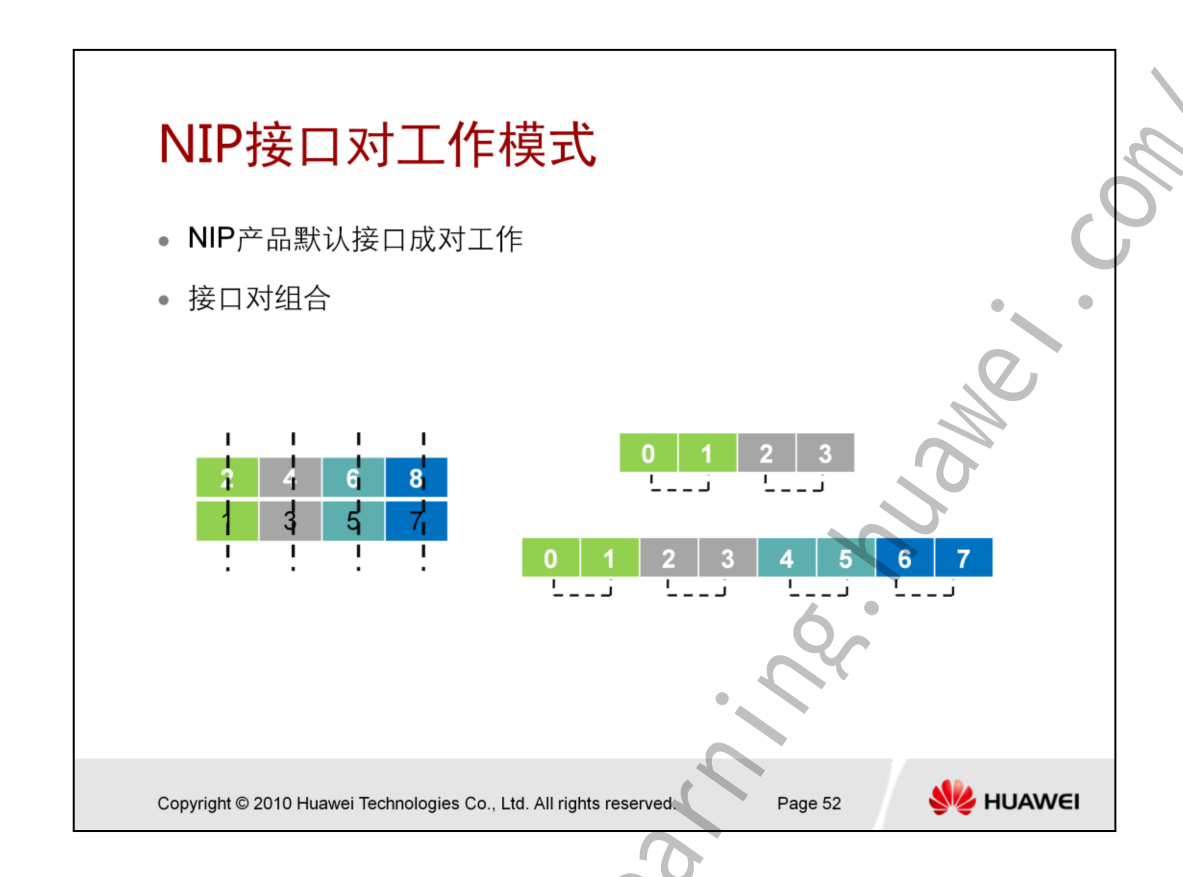




1、PC控制台上可以用于使用sweb控制设备或者安装NIP Manager软件；

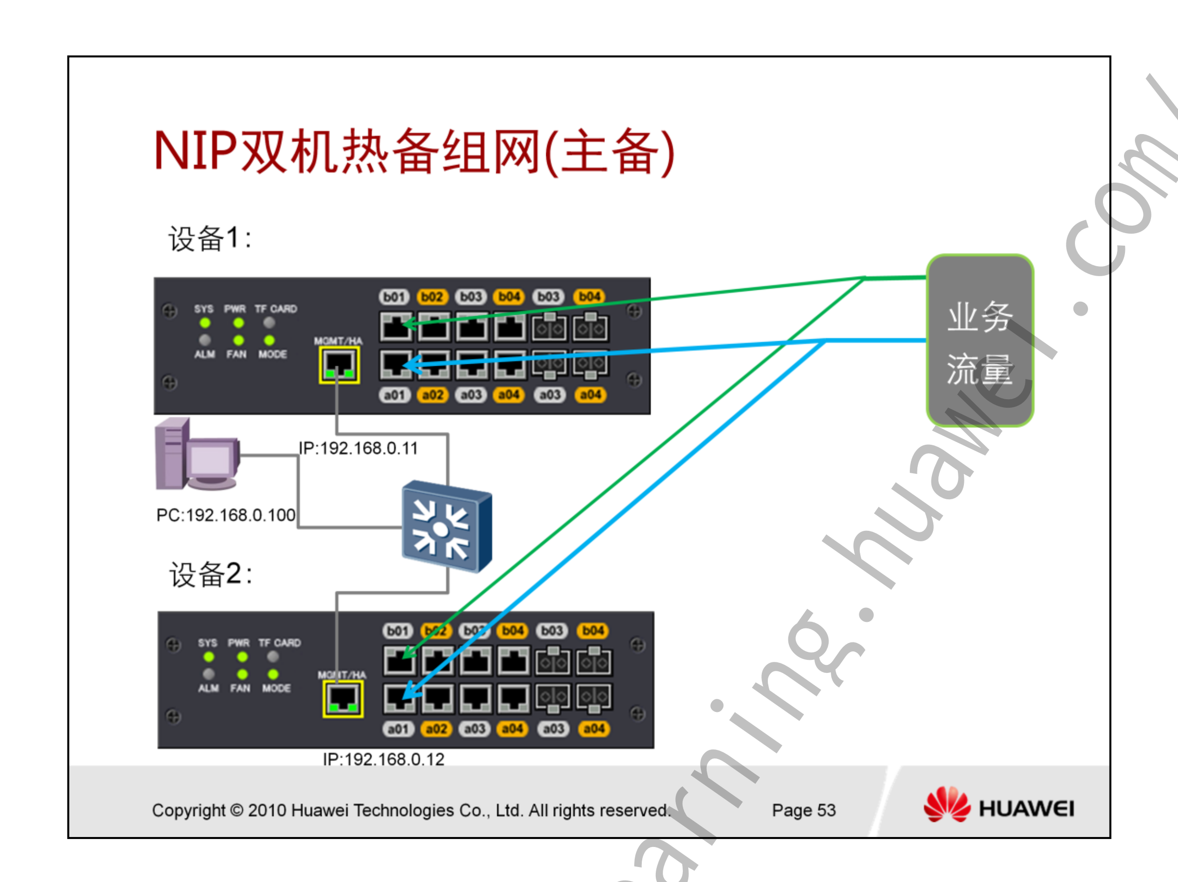
2、sweb控制与NIP Manager可以使用同一个PC控制台，也可以使用两个不同的PC；

将PC配置为192.168.0.XX/ 24与设备联通；登陆sweb进入配置，接口点击配置管理口IP地址、网关、DNS等，使设备可以访问升级服务器；

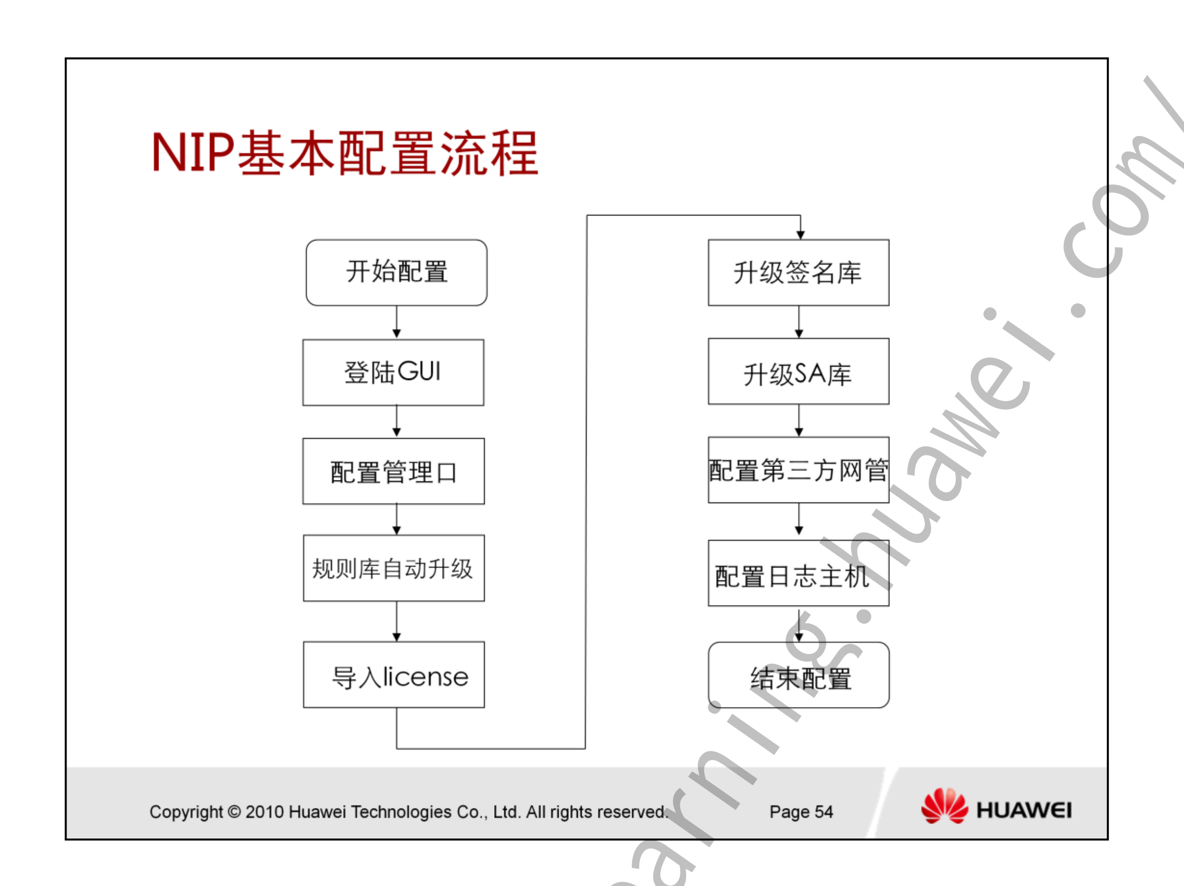


NIP产品默认接口都是成对工作的，包括主接口版和扩展接口卡上的接口都是按接口顺序从前至后，两两成对工作（如a01-b01），默认工作模式为IPS，用户可以根据需要转换为IDS模式；一个接口对内部工作时是共享会话的。

接口对可以根据需要进行组合，形成接口对组合，一个接口对组合内部是共享会话的。



- 建议使用千兆交换机互联；
- 先将一台设备接入交换机，使用sweb登陆一台设备后配置好管理口IP地址、配置为HA主机
- 再将另一个设备接入交换机，配置其IP地址、配置为HA备机
- 将业务流量同时接入相同的业务口



首先需要对控制台进行安装，有关控制台的安装在本胶片中不作详细描述，具体参看NIP的产品安装手册。

NIP基本配置步骤

- 登录GUI
- 查看'威胁防护'策略配置[建议]
- 配置规则库自动升级[建议]
- 导入License[建议]
- 手动升级“入侵防护”规则库[非必须]
- 手动升级“应用控制”知识库[非必须]
- 根据需要进行接口对/组合的配置[非必须]
- 配置第三方网管和日志主机[非必须]



NIP的默认出厂配置，已经为用户考虑了通用场景下，设备的基本配置；也就是说，用户几乎不用做任何的软件设置，NIP就可运行上线进行入侵防护检测。

登录设备

- 将PC的网线连接到IPS设备的Mgmt口上;
- 默认配置下,以192.168.0.1为IP地址进行web登录;用户名为:admin 密码:Admin@123。



HUAWEI

注意:密码区分大小写,默认连续五次输入出错,将被锁定一分钟不能登录;

配置管理口参数

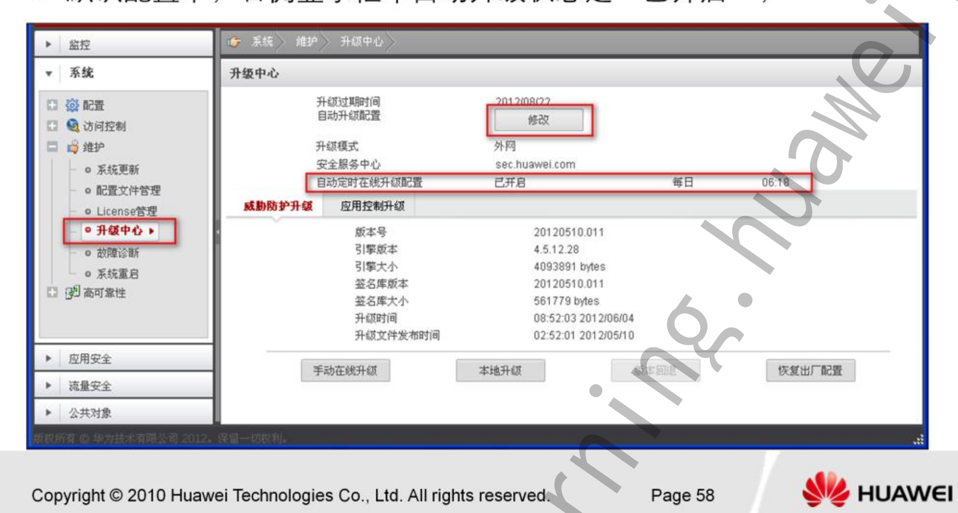
- 左侧菜单样中选择:“系统”→“配置”→“接口配置”；
- 在右侧显示框中，选中面版图上的“MGMT”口，配置其IP、网关、“DNS首选地址”与“DNS备选地址”；





配置规则库自动升级

- 左侧菜单样中选择:“系统” →“维护” →“升级中心”；
- 默认配置下，右侧显示框中自动升级状态是“已开启”；



HUAWEI

左侧菜单样中选择:“系统” → “维护” → “升级中心”；

默认配置下，右侧显示框中自动升级状态是“已开启”；

如果没有开启，请点击“修改”进行配置即可；确认升级过期时间未过期，如果已过期，请导入license或者联系HS用服。

导入License-1

- 新设备上线需要用户需要导入配套的license文件，如果没有导入或者已经过期，系统不能执行IPS、SA升级功能。
- 左侧菜单中选择“系统”→“维护”→“License管理”；
- 在右侧“License文件管理”区域中，点击“上传”按钮，在弹出的对话框中，点击“济览”，选择待上传的License文件；





导入License-2

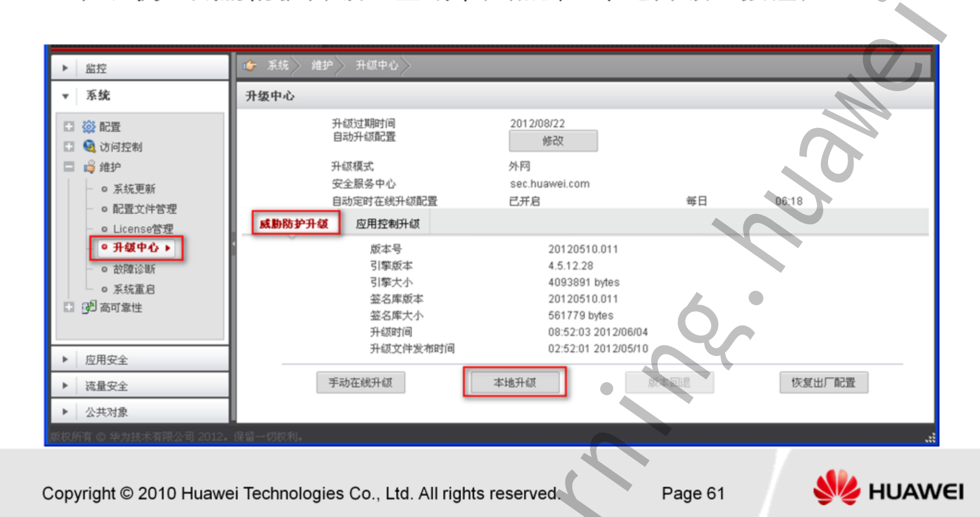
- 上传License文件成功后，点击“配置”对应的小灯泡，即可完成License文件激活；
- 提示：激活后，小灯泡会变亮；





手动升级“入侵防护规则库”

- 左侧菜单中选择“系统”→“维护”→“升级中心”；
- 在右侧“威胁防护升级”区域中，点击“本地升级”按钮；



HUAWEI

在系统\维护\升级中心\威胁防护\ 页面点击 “本地升级”，在升级列表中选择或者上传新的升级文件。

上传升级包成功后，点击“配置”对应的小灯泡，即可完成入侵防护本地规则库升级；

提示：由于升级过程中需要对规则库进行编译操作，整个过程较长，一般需要3~4分钟，请耐心等待。

配置第三方网管

- 系统\配置\第三方网管中配置，支持SNMP V1/V2C/V3版本配置



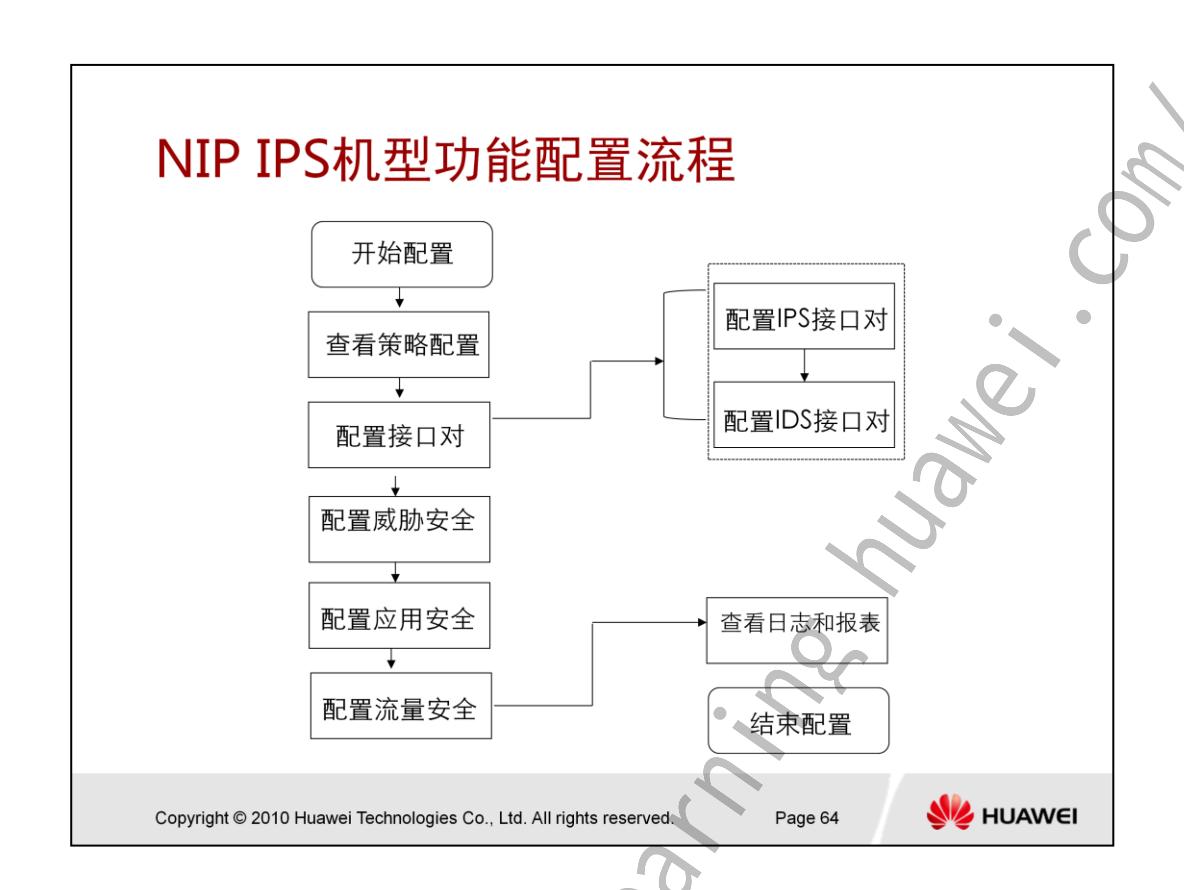


配置日志主机

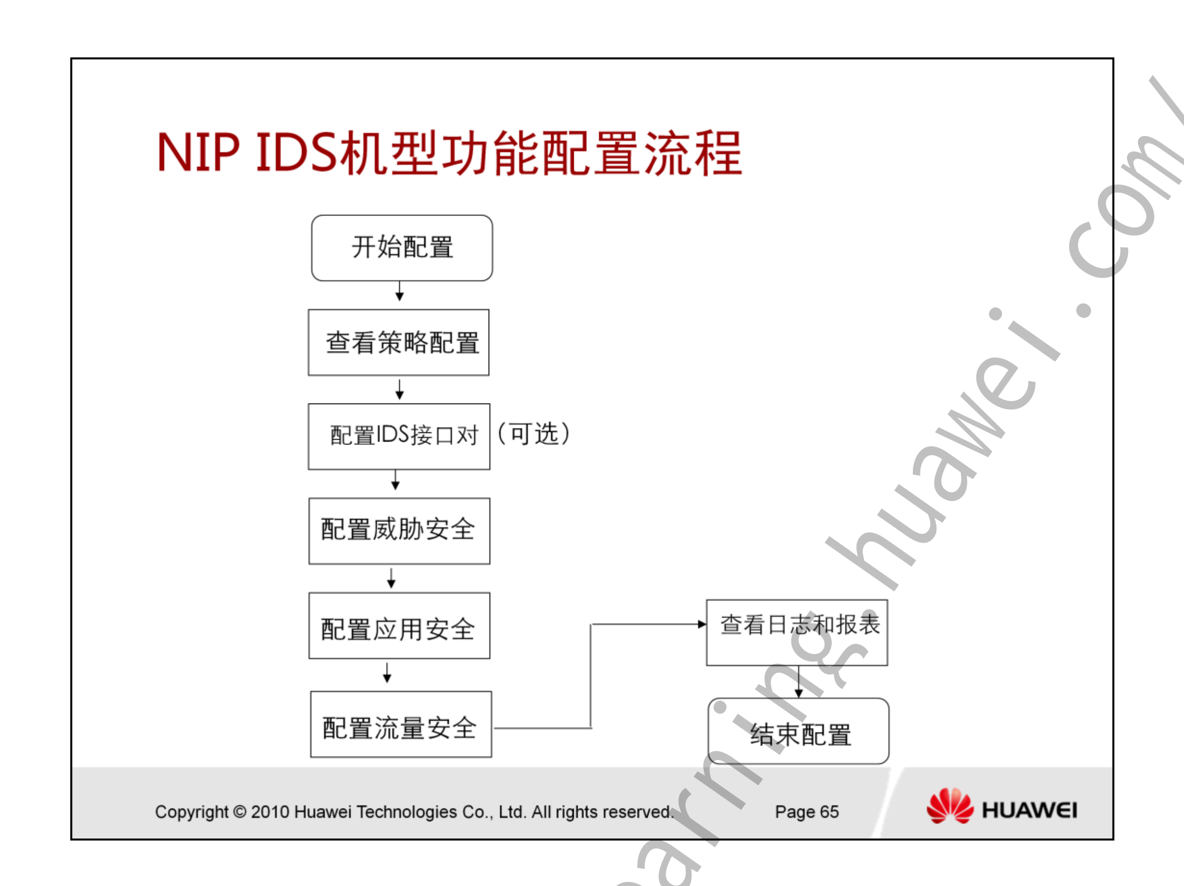
- 系统\配置\日志主机中配置，最多可配置3个日志主机，接收设备发出的日志信息。



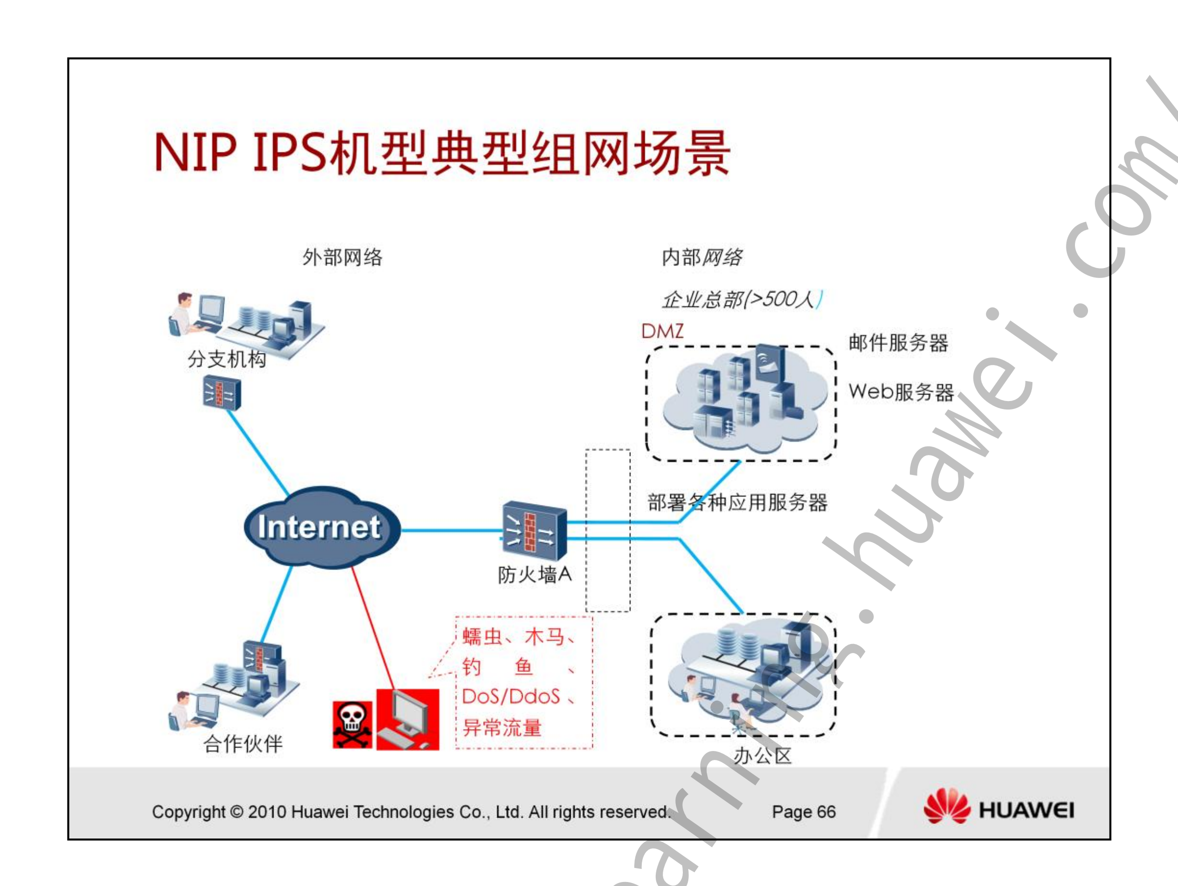




首先需要对控制台进行安装，有关控制台的安装在本胶片中不作详细描述，具体参看NIP的产品安装手册。



首先需要对控制台进行安装，有关控制台的安装在本胶片中不作详细描述，具体参看NIP的产品安装手册。

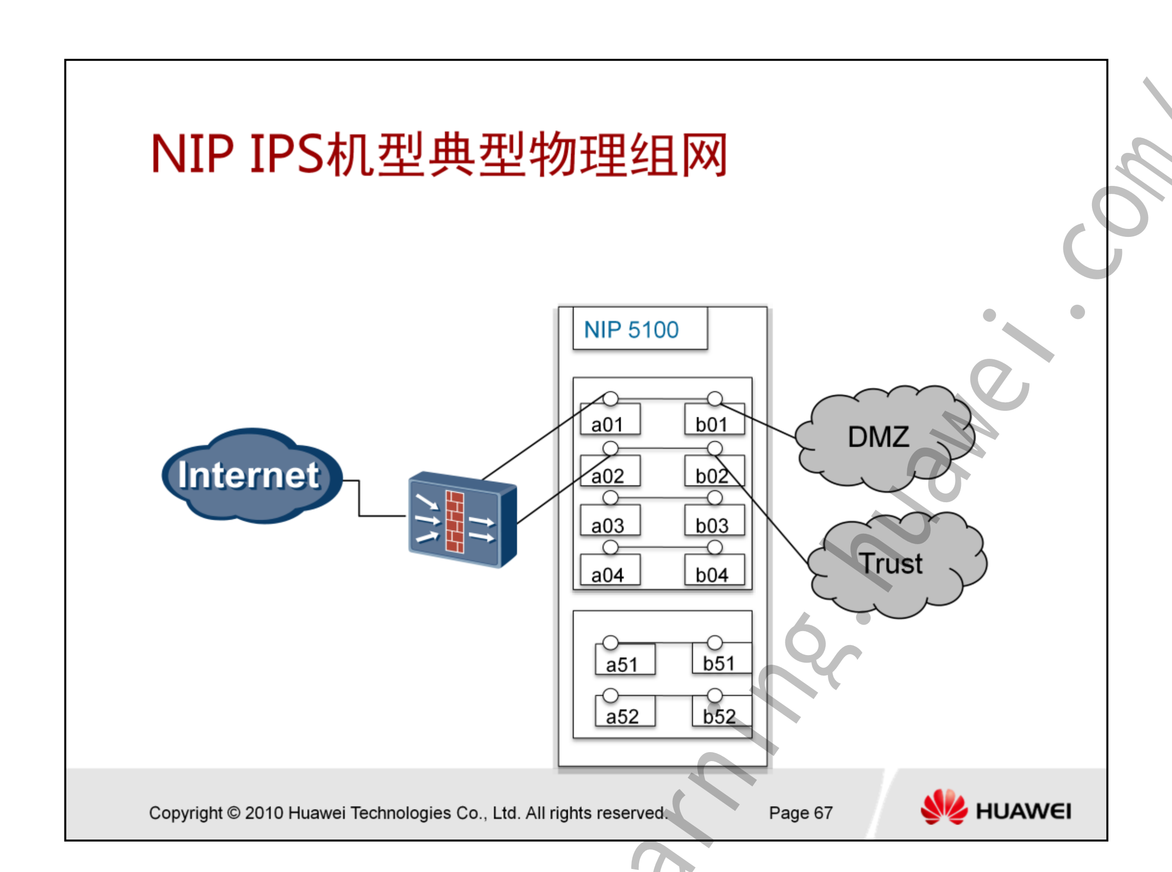


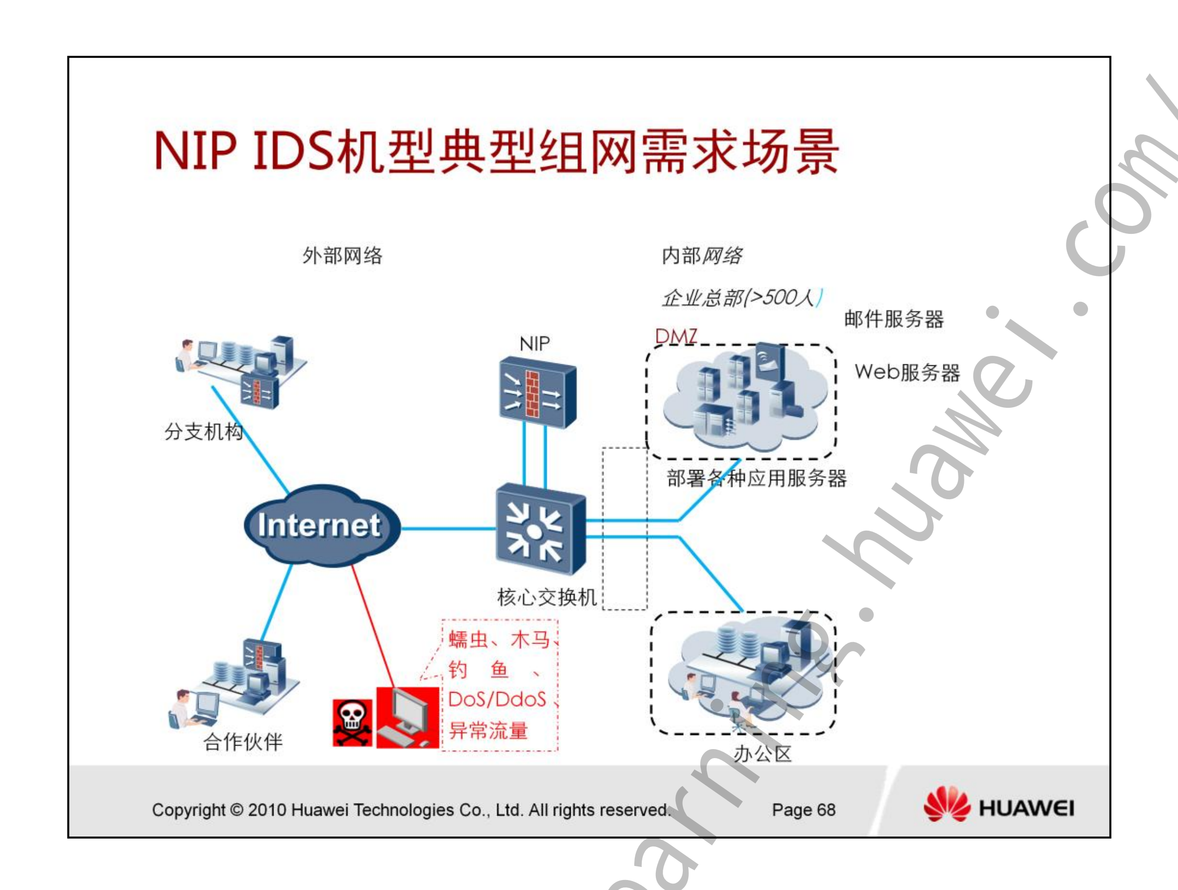
某一中型企业内网与互联网互通。内（dmz）对外发布Web、FTP等服务。

1、服务器需要全面防护，防止来至互联网的各种攻击。

2、需要防止公司总部员工看土豆视频类P2P网络电影、使用QQ、MSN等聊天工具。

3、防护总部办公区，防止黑客、木马、蠕虫等攻击。


NIP IPS机型典型物理组网
NIP 5100
Internet
a01
b01
a02
b02
a03
b03
a04
b04
a51
b51
a52
b52
DMZ
Trust
Page 67
HUAWEI



某一中型企业内网与互联网互通。内（dmz）对外发布Web、FTP等服务。

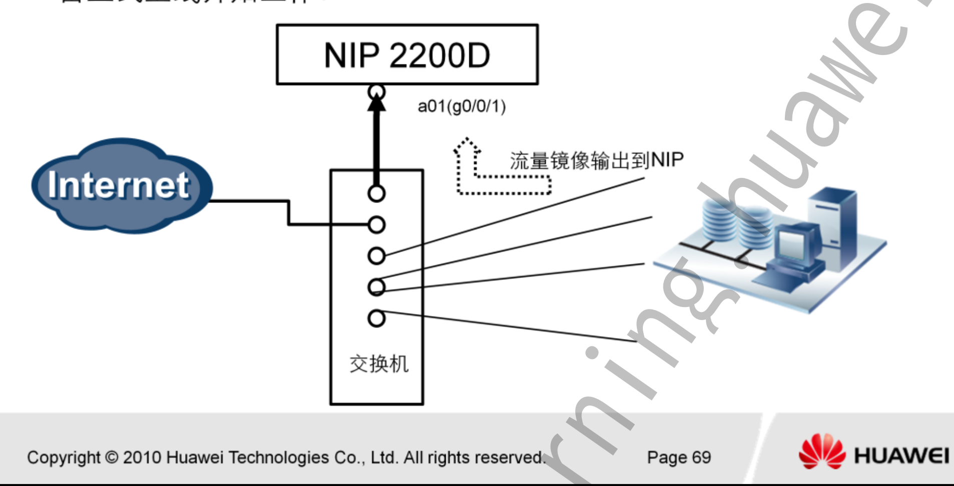
1、服务器需要全面防护，防止来至互联网的各种攻击。

2、需要防止公司总部员工看土豆视频类P2P网络电影、使用QQ、MSN等聊天工具

3、防护总部办公区，防止黑客、木马、蠕虫等攻击

NIP IDS机型典型物理组网

- 首先，需要配置用户交换机，将需要审计的正反向流量都镜像到输出口上，然后使用网线与NIP设备的a01(g0/0/1)口，连接起来，设备正式上线开始工作。



确认引擎版本—威胁防护

HUAWEI NIP5100

系统 > 维护 > 升级中心

升级中心

升级过期时间	2012/08/22
自动升级配置	修改
升级模式	外网
安全服务中心	sec.huawei.com
自动定时在线升级配置	已开启 　每日　04:36

威胁防护升级　应用控制升级

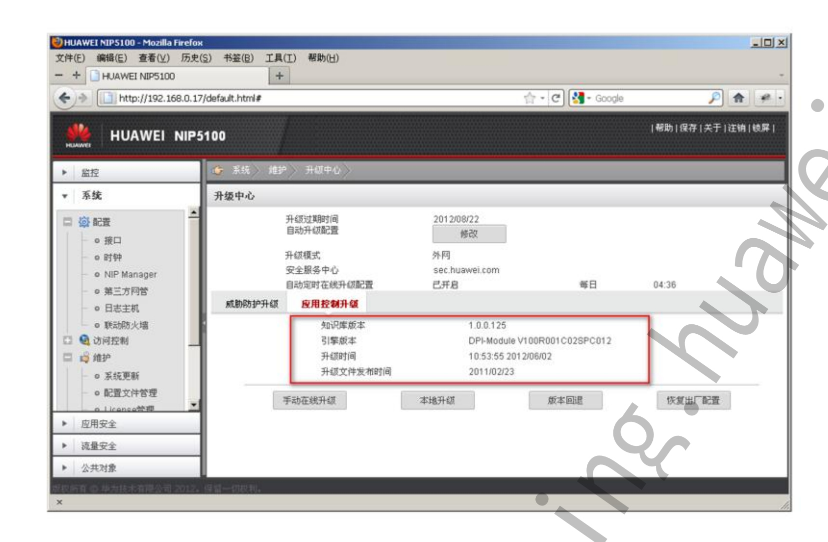
版本号	20120510.011
引擎版本	4.5.12.28
引擎大小	4093891 bytes
签名库版本	20120510.011
签名库大小	561779 bytes
升级时间	10:56:42 2012/06/02
升级文件发布时间	02:52:01 2012/05/10

手动在线升级　本地升级　版本回退　恢复出厂配置

HUAWEI

需要确认此处的各个版本都有具体内容而非0；如果为0，请执行本地升级或者在线升级，确保升级成功。

确认引擎版本—应用控制


HUAWEI NIP5100 - Mozilla Firefox
http://192.168.0.17/default.html#
HUAWEI NIP5100
升级中心
升级过期时间 2012/08/22
自动升级配置
修改
升级模式 外网
安全服务中心 sec.huawei.com
自动定时在线升级配置 已开启 每日 04:36
威胁防护升级
应用控制升级
知识库版本 1.0.0.125
引擎版本 DPI-Module V100R001C02SPC012
升级时间 10:53:55 2012/06/02
升级文件发布时间 2011/02/23
手动在线升级
本地升级
版本回退
恢复出厂配置
监控
系统
配置
接口
时钟
NIP Manager
第三方网管
日志主机
联动防火墙
访问控制
维护
系统更新
配置文件管理
应用安全
流量安全
公共对象

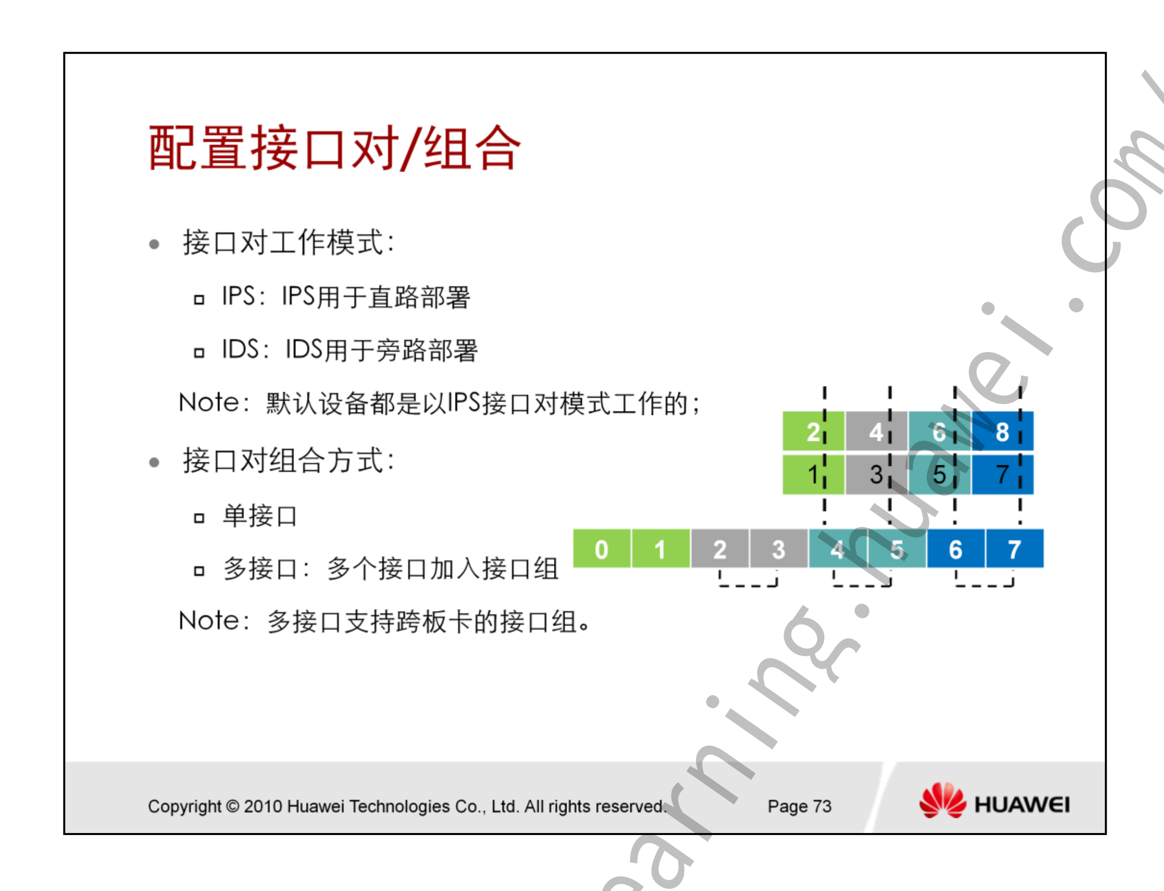


查看策略配置（威胁防护）

- 登录成功后,在左侧菜单样中选择:“应用安全”→“策略应用”，并选择网线接入的接口组，如“a01-b01”；
- 在右侧显示框中，能够看到“a01→b01”与“b01→a01”两个方向都应用了“威胁防护”策略“default”；







接口对工作模式分为IPS、IDS两种；IPS用于直路部署、IDS用于旁路部署；默认设备都是以IPS接口对模式工作。

接口对模式可以转换，用户可以根据需要在IPS、IDS模式直接互转；用户在使用设备前应该根据网络实际情况进行分析，选择合适的方式。

在有特殊要求（负载均衡链路或者来回路径不一致链路）中可以配置接口对组合来满足用户需求；

- 接口对组合是以接口对为单元的组合，不同于接口的聚合；
- 用户可以将2个或者更多的接口加入接口对组合；
- 系统支持跨板卡的接口对组合。
- 接口对组合的配置是整体性的，应用策略和查看流量等都以组合作为一个整体单位。

配置接口对/组合

- 用户可以对组合好的接口对进行转换工作模式、修改别名或者删除组合等满足操作。





配置接口对/组合

- 勾选将要组合的接口对，然后点击组合，选择工作模式、输入别名后，创建组合。

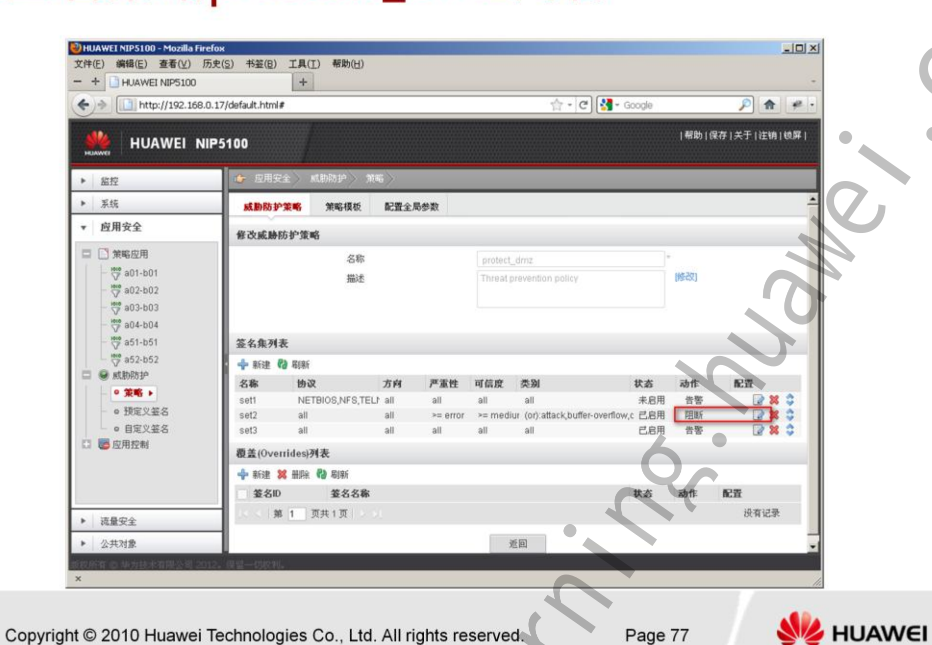


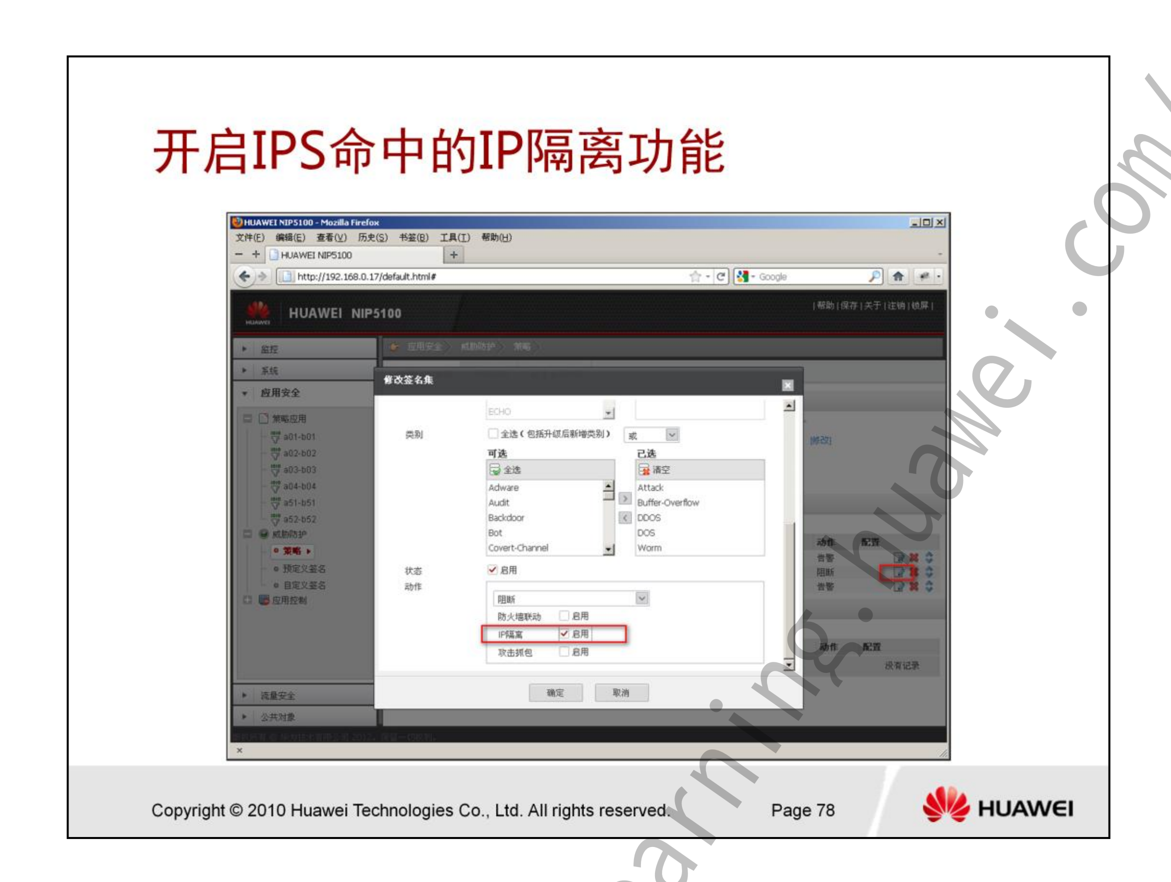


创建威胁防护策略


HUAWEI NIP5100 - Mozilla Firefox
文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)
HUAWEI NIP5100
http://192.168.0.17/default.html#
HUAWEI NIP5100
| 帮助 | 保存 | 关于 | 注销 | 锁屏 |
监控
系统
应用安全
策略应用
a01-b01
a02-b02
a03-b03
a04-b04
a51-b51
a52-b52
威胁防护
策略
预定义签名
自定义签名
应用控制
流量安全
公共对象
应用安全 威胁防护 策略
威胁防护策略
策略模板
配置全局参数
新建威胁防护策略
名称
protect_dmz
描述
Threat prevention policy
同步策略/策略模板
dmz
应用
返回

查看策略protect_dmz内容





根据用户需求，配置set2的阻断行为，在开启在IPS命中后进行IP隔离开关；

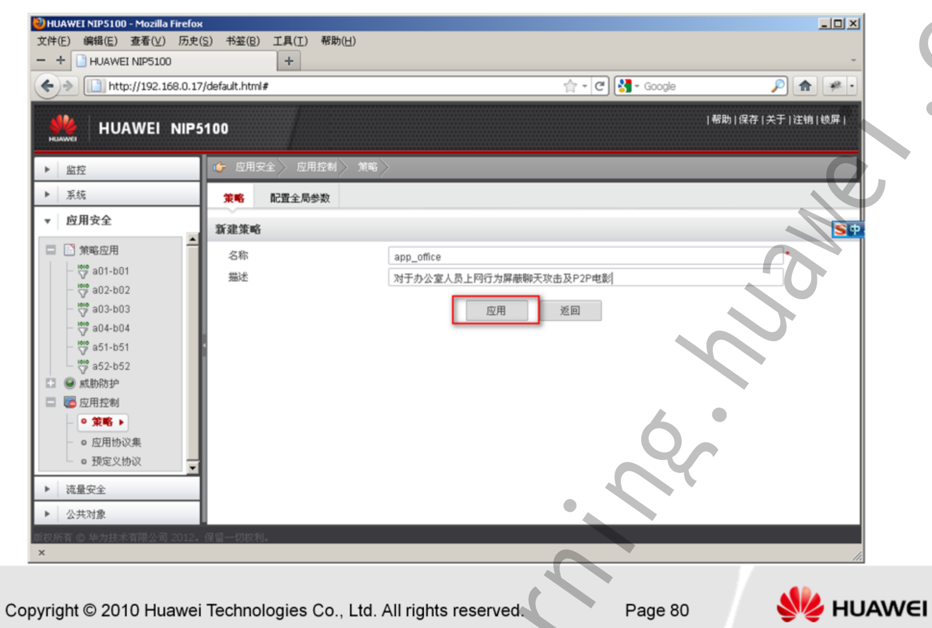
如果用户需要进行防火墙联动也可以类此配置。

查看策略protect_dmz修改后内容



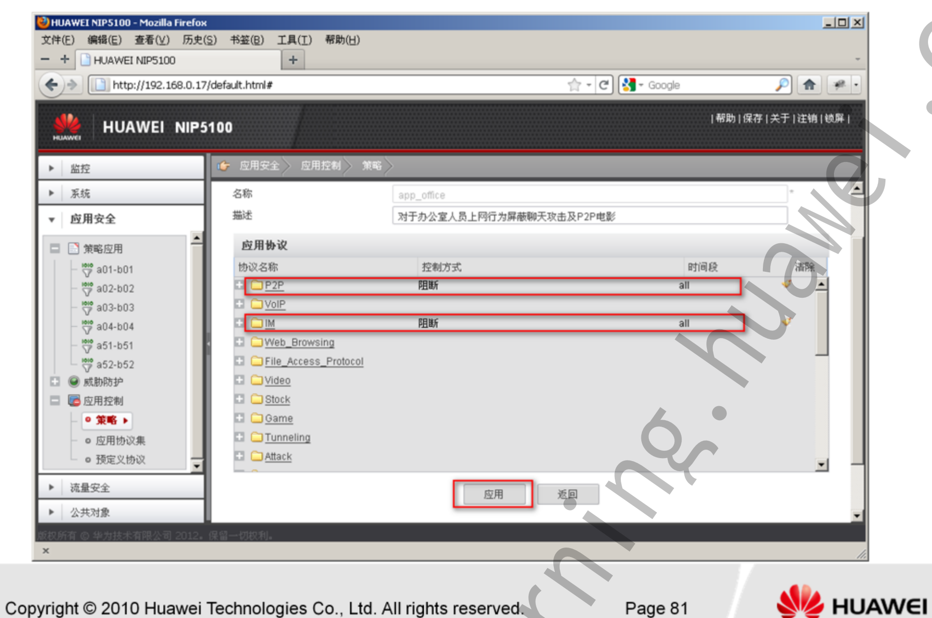


新建应用控制策略app_office



HUAWEI

配置P2P、IM阻断结果



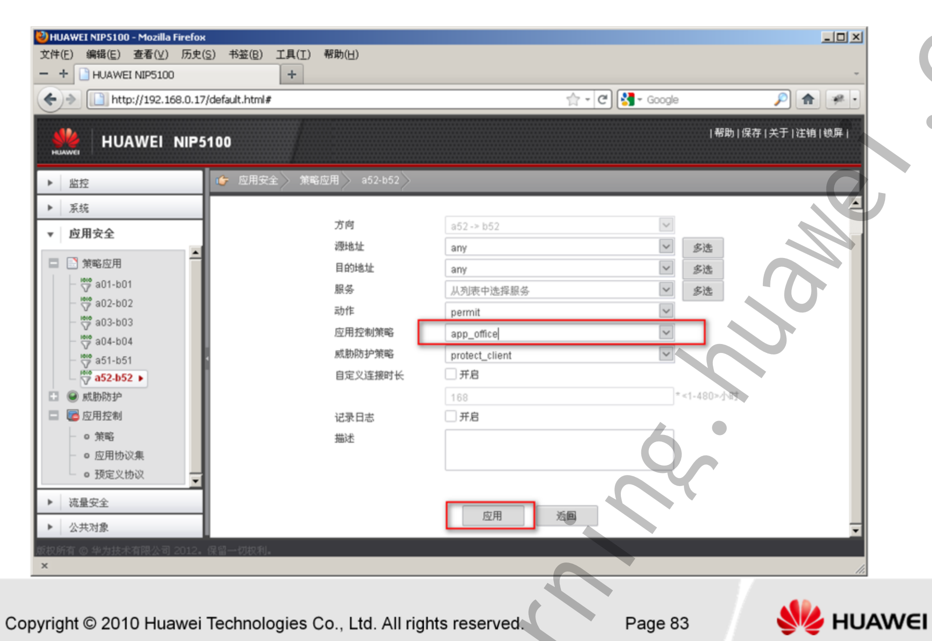
HUAWEI

统一编译



确认
1
策略修改后需要提交才能生效，请确认是否立即提交？如果有多条策略需要修改可以选择“否”，后续在威胁防护策略列表中统一提交。
是
否
2
编译进行中，请耐心等待！
统一编译
提示
3
提示：提交成功。
确定

在策略应用中引用应用控制策略



HUAWEI

查看应用策略结果

HUAWEI NIP5100 - Mozilla Firefox

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

HUAWEI NIP5100

http://192.168.0.17/default.html#

HUAWEI NIP5100 | 帮助 | 保存 | 关于 | 注销 | 锁屏 |

监控
系统
应用安全
- 策略应用
  - a01-b01
  - a02-b02
  - a03-b03
  - a04-b04
  - a51-b51
  - a52-b52
- 威胁防护
- 应用控制
  - 策略
  - 应用协议集
  - 预定义协议

流量安全
公共对象

应用安全 > 策略应用 > a52-b52

策略列表

新建 删除 清除全部命中次数 刷新 全部 查询 高级查询

ID	源地址	目的地址	服务	动作	应用控制策略	威胁防护策略	描述	命中次数	启用	配置
a52 → b52 (2 Items)										
1	any	any	ip	permit	app_office	protect_client	--	0	☑	
0	any	any	ip	permit	--	default	--	0	☑	
b52 → a52 (2 Items)										
1	any	any	ip	permit	app_office	protect_client	--	0	☑	
0	any	any	ip	permit	--	default	--	0	☑	

第 1 页共 1 页　　显示 1 - 4，共 4 条



启用SYN Flood攻击防御

HUAWEI NIP5100 - Mozilla Firefox

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

HUAWEI NIP5100

http://192.168.0.17/default.html#

HUAWEI NIP5100

| 帮助 | 保存 | 关于 | 注销 | 锁屏 |

监控
系统
应用安全
流量安全
流量型
全局参数配置
TCP Flood
TCP连接耗尽
UDP Flood
HTTP Flood
HTTPS Flood
DNS Flood
SIP Flood
ICMP Flood
报文型
公共对象

流量安全 > 流量型 > TCP Flood

配置TCP Flood攻击防御

☑ SYN Flood攻击防御

防御模式 ◉ 基本 ○ 增强

包速率阈值 2000 <1-1200000>包/秒

☐ SYN-ACK Flood攻击防御

☐ ACK Flood攻击防御

☐ TCP分片攻击防御

☐ FIN/RST Flood攻击防御

☐ TCP限流

应用





根据实际网络情况，开启基线流量学习功能，并设置学习周期；设置是否自动应用学习成果；基线学习功能是用户可选配置。



通过勾选将配置的流量安全配置应用到相应接口上。


查看检测结果—统计
HUAWEI NIP2200D - Mozilla Firefox
HUAWEI NIP2200D
威胁防护统计
威胁防护攻击
TOP10
异常流量统计信息
威胁防护严重性统计信息
大类应用协议比例统计信息
威胁防护攻击事件TOP10
设备资源信息
告警信息
监控
状态
日志
IP隔离
系统
应用安全
流量安全
公共对象
Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.
Page 88
HUAWEI

查看攻击日志

HUAWEI NIP2200D - Mozilla Firefox

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

HUAWEI NIP2200D

http://192.168.0.5/default.html#

HUAWEI NIP2200D

| 帮助 | 保存 | 关于 | 注销 | 锁屏 |

监控

状态

日志

IP隔离

系统

应用安全

流量安全

公共对象

监控 > 日志

输出日志的级别 警告 应用

日志显示列表

导出 刷新 日志类型 威胁防护 查询 高级查询

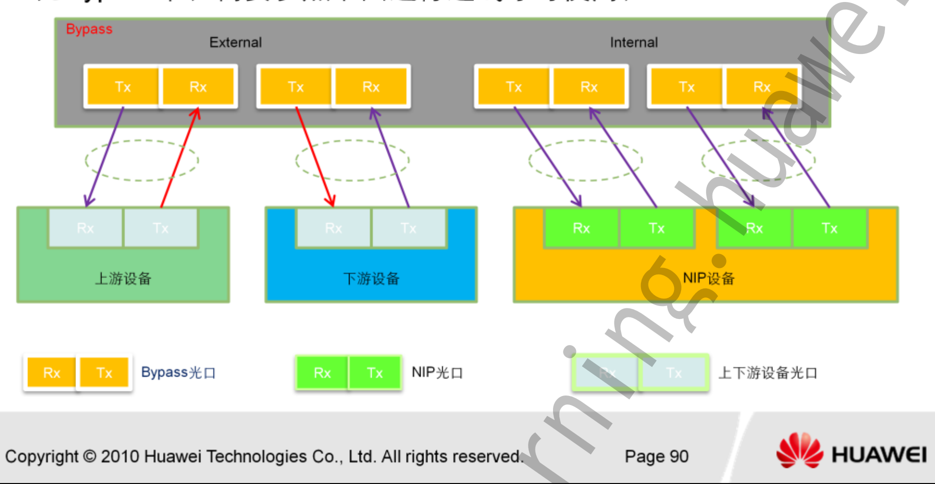
安全级别	日志类型	时间	描述	配置

第 1 页共 1 页 没有记录



Bypass卡的使用

- 电Bypass卡，直接作为业务口使用，使用方法与普通业务接口无区别。
- 光Bypass卡，需要参照下图进行连线才可使用；



- Bypass光口：Bypass卡上的一路光口（四对收发）

  一般光Bypass卡，都是两路或两路以上的。Bypass卡需要插在NIP设备某个slot槽位上。External下的两队接口用于连接上下游设备，而Internal下发的接口用于与NIP设备上的通信口连接。

- NIP光口：NIP设备上的光口。

  这些光口可以是主接口面板上的光口，也可以是用户插入的光接口卡。

- 上下游设备光口：用于连接上下有设备，接入流量使用。

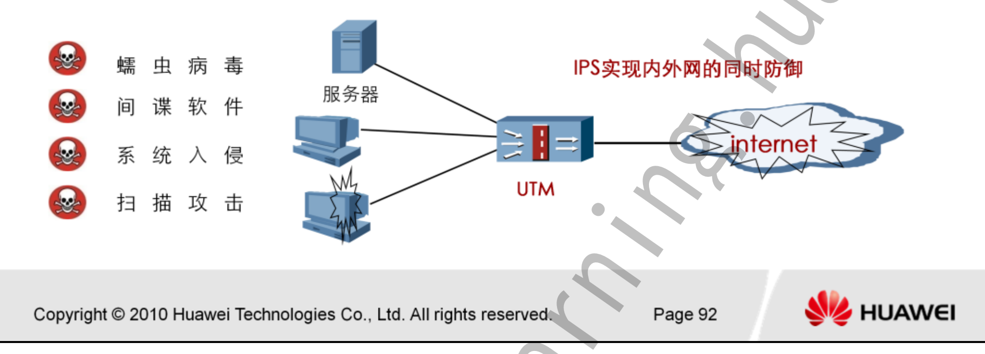


目录

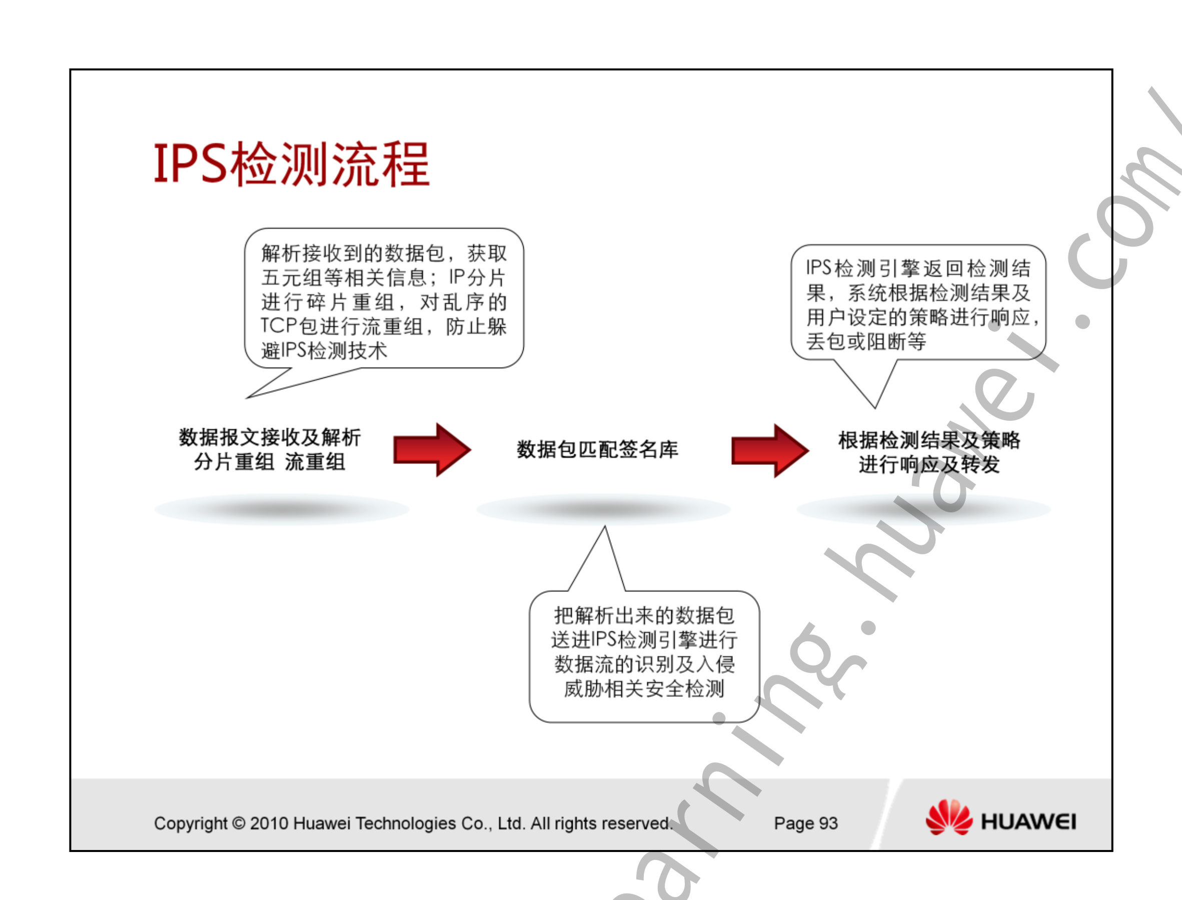


IPS功能介绍

- 防范针对应用漏洞发起的入侵攻击，如针对IE漏洞，Outlook漏洞，SQL数据库漏洞，系统漏洞等；
- 对恶意程序攻击行为的检测，如蠕虫，木马，间谍软件的攻击行为等；
- 对可疑的网络行为进行检测，包括文件共享，远程控制等；
- 对非法操作的检测，如对扫描的检测；
- 防范零日攻击。



- 对知名协议的有效识别
  - 由于有些知名的应用协议并非开在知名的服务端口上，如HTTP服务可能开在8080端口，原先基于端口号进行协议识别的方法就会失效，导致一些安全检测被遗漏了；
  - USG5000能够识别HTTP,SMTP,FTP,POP3,IMAP4,MSRPC,NETBIOS,SMB,MS_SQL,TELNET,IRC,QQ,ICQ,Google Talk,Yahoo Messenger,eMule, eDonkey协议。
- 对协议异常的分析
  - 知名的应用协议是有一套公认的标准，如某个字段的数据长度最大为多少，如：DNS域名解析请求中，域名每节的字符长度不能够超过63，超过了则可能导致某些DNS服务器出错等；
  - USG5000能够对HTTP,SMTP,FTP,POP3,IMAP4,MSRPC,NETBIOS,SMB,MS_SQL,TELNET,IRC, DNS协议进行协议异常分析。



对入侵行为进行响应，丢包及阻断(这是常规的响应方式，有的产品可能还支持其它响应方式，如邮件告警等)提供日志记录和报表功能，方便企业对于网络安全状况的了解和取证。



目录



IPS典型组网配置

步骤一：IPS基础配置

- 步骤1.1 License激活
- 步骤1.2 IPS引擎加载（升级）
- 步骤1.3 IPS全局配置

步骤二：IPS策略配置应用

- 步骤2.1 创建并配置IPS策略
- 步骤2.2 应用IPS策略



- 在进行IPS模块的配置前，需要完成以下三个预配置：
  - DNS配置。只有配置了才能解析sec.huaweisymantec.com升级特征库。
  - UTM运行模式的全局配置，出厂默认工作在防火墙模式，需要通过命令runmode utm，更改为UTM运行模式。
  - 大流量下业务优先、安全优先的配置。

执行命令utm bypass enable，启用深度检测过载保护功能。 缺省情况下，启用深度检测过载保护功能。启用深度检测过载保护功能将实现业务优先。当USG出现内存不足或者CPU处理能力达到上限的情况下，UTM功能自动短暂失效，报文不经过UTM功能的检测就被转发。当USG的内存使用情况和CPU处理能力恢复正常后，UTM功能将自动生效。

IPS基础配置—License激活上传

点击"浏览"按钮，以上传License文件

输入License授权编码，保证设备已经连接Internet，点击激活。设备将自动下载License到设备中。

- 本地手动激活：已经通过License平台获取到License文件的情况。
- 在线自动激活：已经购买License，并获取License授权编码。（推荐）

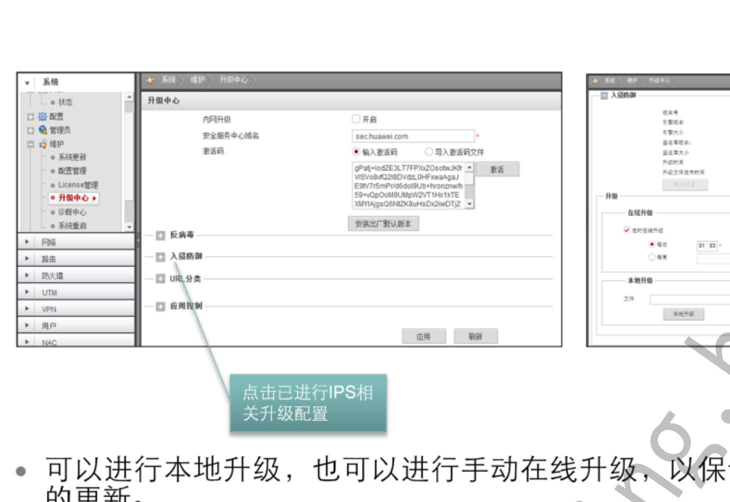
 Page 96 HUAWEI

License用来动态控制产品的某些特性是否可用。利用License机制，可以灵活地根据客户的需求增减特性，保护并节省用户的投资。

- 合同编号（Contract No.）：从License授权证书上获得；
- License授权码LAC（License Authorization Code）：从License授权证书上获得；
- 设备序列号ESN（Equipment Serial Number）：登录到设备web界面后，展开"系统 > 维护 > License管理"，在"防火墙License信息"界面上可获得设备序列号ESN。

注：系统中只能存在一个处于激活状态的License文件，激活新的License将会使旧的License失效 。

IPS基础配置—IPS引擎升级设置




点击已进行IPS相关升级配置

- 可以进行本地升级，也可以进行手动在线升级，以保证特征库引擎的更新。



- IPS引擎根据特征库进行监测，需要保证IPS引擎更新到最新的特征库；
- USG5000提供定时在线升级、手动在线升级、本地升级三种升级方式，灵活实现IPS引擎和签名库、AV反病毒引擎和病毒库的更新；
- 用户可以选择先下载IPS版本，确认后再进行安装或者下载后直接安装的方式。缺省情况下，需确认后再进行安装。选择此方式后，定时在线升级、手动在线升级和本地升级均只将IPS版本下载到USG上，不安装。只有当USG上存在新下载的IPS版本时，“安装升级包”按钮才生效；
- 手动安装需要在sec.huaweisymantec.com注册下载签名库的时候获取激活码。

IPS基础配置—IPS全局设置

UTM > 基本配置 > 基本配置
基本配置
UTM功能 启用 应用
只有启用UTM功能并且有相应的License时，入侵防御、反病毒、URL过滤和垃圾邮件过滤功能才可以使用。
全局启用UTM功能

UTM > 入侵防御 > 策略
IPS策略 策略模板
配置全局参数
入侵防御功能开关 启用
工作模式 防护模式
特权策略 ---- NONE ----
应用
全局启用IPS功能

 Page 98 HUAWEI

使用IPS功能前，请先全局启用IPS功能并配置IPS的工作模式，另外，USG5000还支持配置特权策略。

- IPS开关

自动启用IPS功能后，匹配防火墙策略的报文将进行IPS扫描。禁用IPS功能后，所有报文都不进行IPS扫描。缺省情况下，USG5000启用IPS功能。

- 工作模式

IPS工作模式有防护模式和告警模式两种。只有在防护模式下，IPS策略中配置的阻断响应方式才可以生效；告警模式下，IPS策略中配置的阻断响应方式无效，即使报文命中的签名对应的响应方式为Block，USG5000也只会产生告警。缺省情况下，IPS工作模式为防护模式。

- 特权策略

当网络中某一类攻击集中爆发时，需要使用统一的策略应对；当这类攻击过去，需要恢复原来配置的策略。USG5000通过配置特权策略实现该功能。

配置了特权策略后，特权策略将替换所有已经应用在域内或域间的策略，没有应用IPS策略的域内或域间不会添加特权策略。取消特权策略配置后，将恢复域内或域间原来的策略配置。

- 以下两种情况会触发USG5000编译IPS策略：
  - 将某条IPS策略配置为特权策略，如果该条IPS策略没有编译或者自上次编译后有修改，会触发USG5000编译所有IPS策略；
  - 取消特权策略的配置时，如果某条IPS策略没有编译或者自上次编译后有修改，会触发USG5000编译所有IPS策略。

IPS策略配置—创建IPS策略

UTM > 入侵防御 > 策略

IPS策略 | 策略模板

配置全局参数

入侵防御功能开关 ☑ 启用
工作模式 防护模式
特权策略 ----- NONE -----
应用

入侵防御策略列表

新建 刷新

名称	引用次数	描述

USG5000提供IPS策略模板，模板中已定义签名集及响应方式。如果模板能够满足应用场景或者与应用场景相似，则可直接在策略中引用模板或引用模板后对签名集进行相应的修改。这样可以达到攻击检测率及性能最优化。

- USG5000提供两个策略模板：
  - Default，default模板包括匹配特定过滤条件的签名，状态为启用，响应方式为Block。该模板能够检测攻击并进行防御，可以应用在一般的入侵防御场景中。说明：使用default模板能够检测并防御的攻击类型包括attack，worm，DoS，DDoS，buffer overflow。
  - IDS，IDS模板包括所有签名，状态为启用，响应方式为Alert。该模板能够检测攻击，但不进行防御，可以应用在一般的入侵检测场景中。



创建IPS策略后，用户可通过配置签名集，以及签名集的启用状态和响应方式来满足特定需求。

- 创建一个签名集后，缺省情况下所有预定义签名都包含在该签名集中。用户需要以下操作过滤签名集中包含的签名：
  - 在签名集中启用某个过滤条件。
  - 配置该过滤条件的过滤参数。
  - 一个签名必须同时满足所有过滤条件才能加入签名集。
  - 包括引用策略模板生成的签名集在内，USG5000一条策略中最多支持10个签名集。

签名集之间存在优先关系，在同一条IPS策略中，排在前面的签名集比排在后面的签名集的优先级高。如果一个签名包含在一条IPS策略的多个签名集中，则USG5000按照优先级高的签名集所配置的启用状态和响应方式对匹配签名的报文进行处理。当安全威胁发生变化，用户可以调整签名集的优先级来满足新的安全需求。

IPS策略中配置签名集后，还可以通过配置覆盖签名满足用户的特殊需求。

IPS策略配置—创建签名集



HUAWEI

IPS策略配置—签名集详细配置

新建签名集

名称 protect_all *

方向 启用 去服务端 去客户端 任意方向

严重性 启用 大于等于 告警

可信度 启用 大于等于 中

协议 启用

可选 AFP AIM DHCP DNS FTP GTP 已选

类别 启用 或

可选 Adware 已选

确定 取消

配置名字，可以凸显该签名集特点

开启类别维度筛选，并选择或的逻辑关系以选择所有签名

最后点击应用以使配置生效

HUAWEI

签名集中只包含预定义签名，不包含自定义签名。

USG5000一条策略中最多支持10个签名集。

签名集之间存在优先关系，在同一条IPS策略中，排在前面的签名集比排在后面的签名集的优先级高。如果一个签名包含在一条IPS策略的多个签名集中，则USG5000按照优先级高的签名集所配置的启用状态和响应方式对匹配签名的报文进行处理。当安全威胁发生变化，用户可以调整签名集的优先级来满足新的安全需求。

IPS策略中配置签名集后，还可以进一步配置覆盖签名来满足用户的特殊。

IPS策略配置应用—域间新建IPS策略

防火墙 > 安全策略 > 转发策略

转发策略列表

新建 删除 刷新 | trust --> untrust 查询 | 高级查询

ID	源地址	目的地址	用户	服务	时间段	动作
untrust->trust						
默认	any	any	any	ip	all	deny
trust->untrust						
默认	any	any	any	ip	all	deny
dmz->trust						
默认	any	any	any	ip	all	deny
trust->dmz						
默认	any	any	any	ip	all	deny
untrust->dmz						
默认	any	any	any	ip	all	deny
dmz->untrust						
默认	any	any	any	ip	all	deny

选择trust和untrust域间关系

新建一个策略以引用IPS策略

配置IPS策略后，把该策略应用到域内或域间后IPS功能才生效。

IPS策略配置应用—域间应用IPS策略

防火墙 > 安全策略 > 转发策略

源安全区域 trust
目的安全区域 untrust
源地址 请选择或输入IP地址 多选
目的地址 请选择或输入IP地址 多选
用户 请选择或输入用户或用户组 多选
服务 请选择服务 多选
时间段 all
动作 permit
描述

☑IPS
IPS策略 protect
☐AV
☐Web过滤
☐邮件过滤
☐FTP过滤
☐应用控制
☐记录日志
☐开启策略会话流量统计

应用 返回

源目的地址不用配置，默认为所有IP报文

动作必须为permit，意思为容许配置IPS策略

勾选IPS，并选择IPS策略protect

点击应用生效

HUAWEI

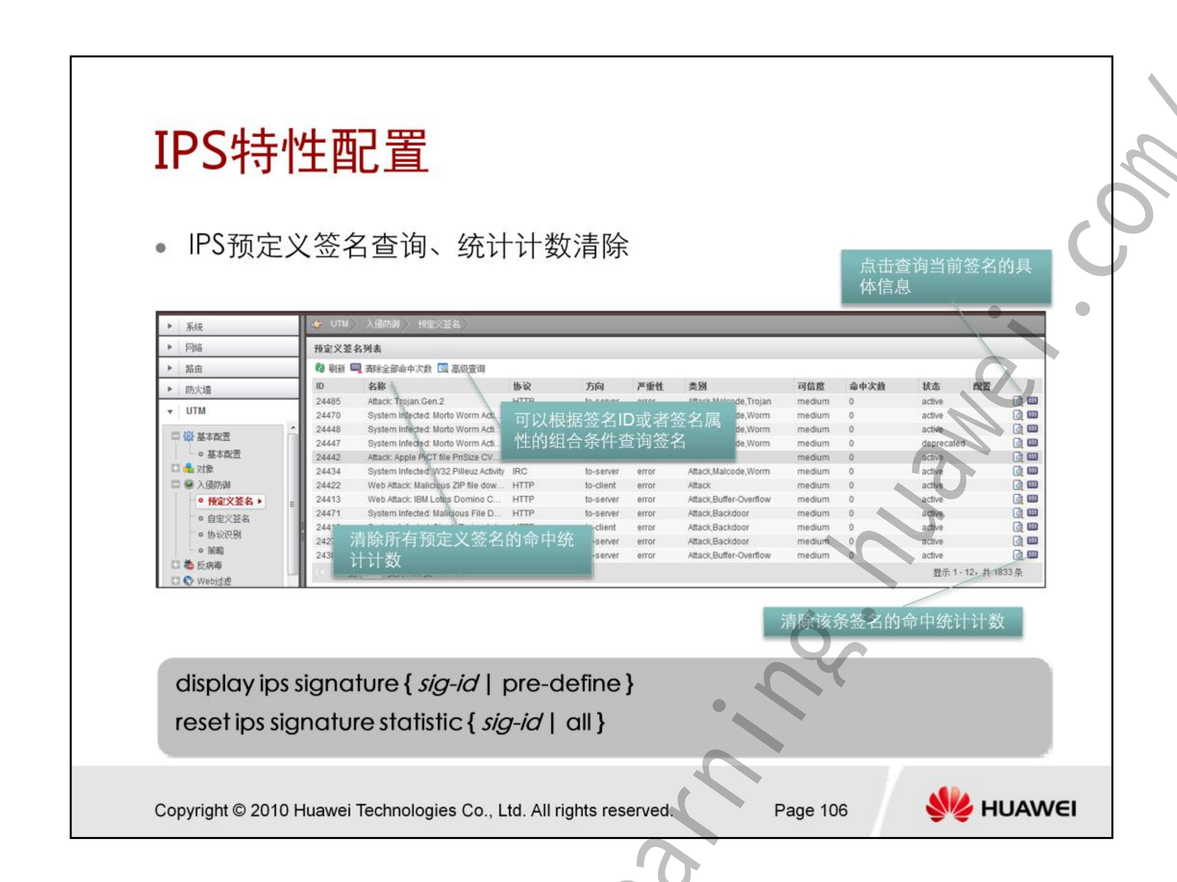
域内或域间应用IPS策略时，如果该条IPS策略没有编译或者自上次编译后有修改，会触发USG5000编译所有IPS策略。

USG5000不支持在Local域内和包含Local的域间应用IPS策略。



目录





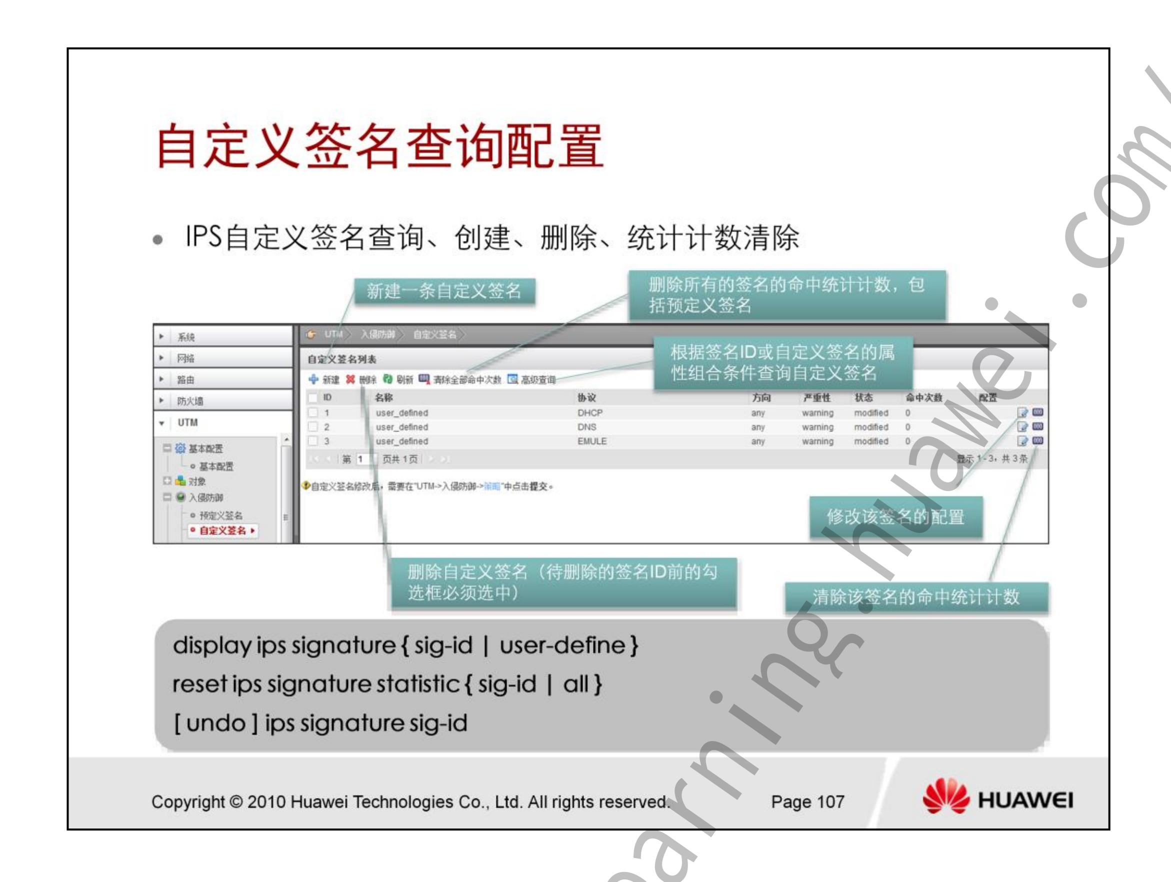
- 预定义签名

包含在USG5000 自带的签名库中，涵盖了网络上大多数蠕虫病毒、木马、间谍程序的入侵特征。预定义签名出厂时保存在USG5000 中，可以通过升级IPS 版本来更新。大约2000条左右。通过命令或web可查看签名的基本信息，不能查看具体的特征码。

命令：display ips signature pre-define

- 自定义签名

用户已知某类攻击依靠预定义签名无法检测出，可根据攻击报文的特征及实际网络情况编写自定义签名，从而快速个性地阻挡攻击。最多支持256条自定义签名。

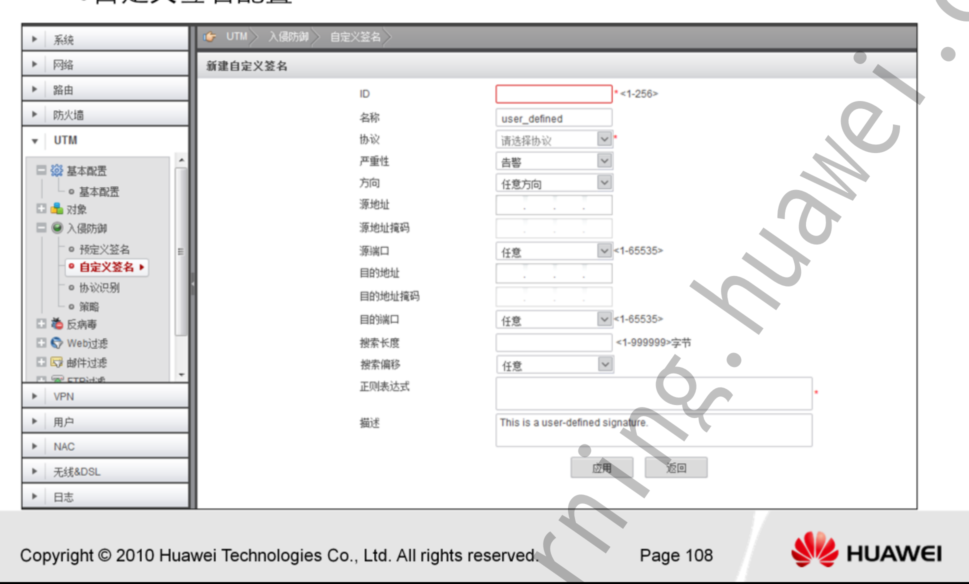


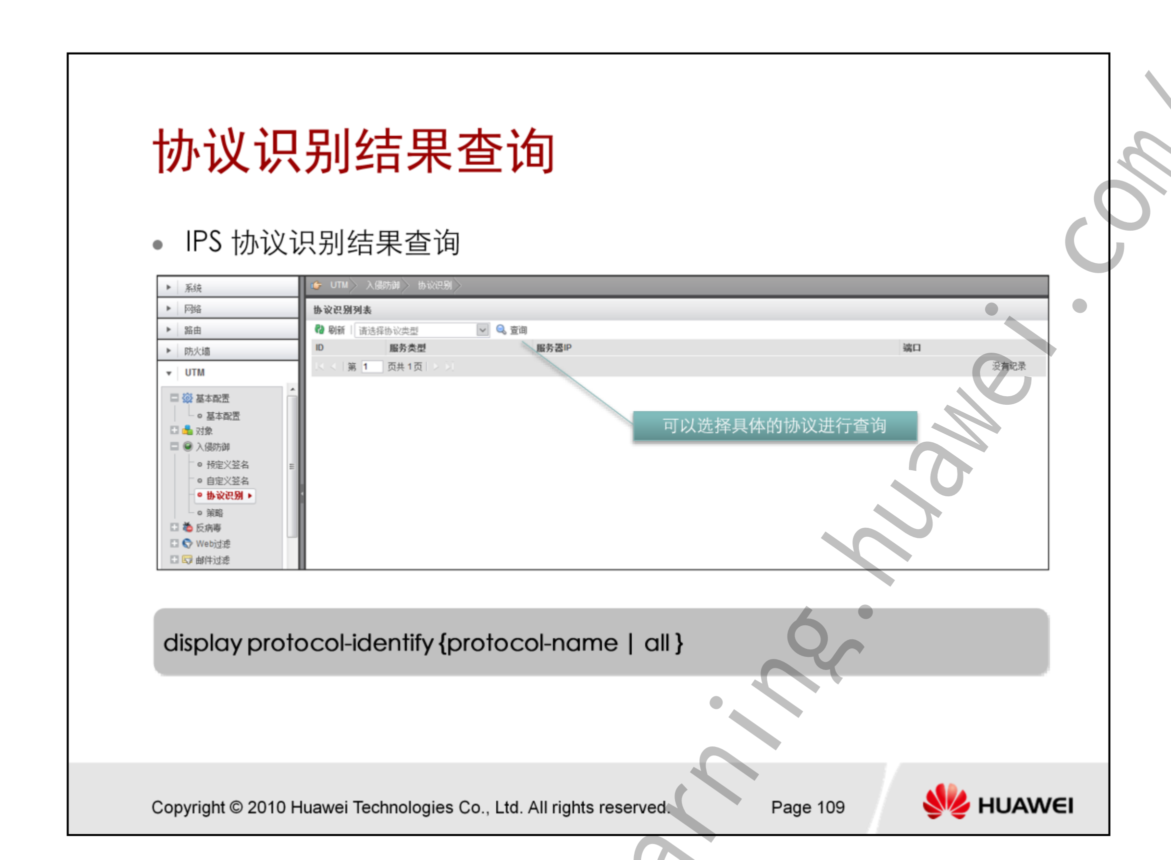
USG5000支持查看自定义签名的协议、方向、严重性和被命中的次数等信息，另外还可以通过查询操作来查看满足指定条件的自定义签名的信息。

- USG5000提供以下两种自定义签名的查看方式：
  - 查看所有自定义签名列表。
  - 查看满足指定查询条件的自定义签名列表，查询条件包括按ID查询和按组合条件查询。

自定义签名配置

- IPS自定义签名配置





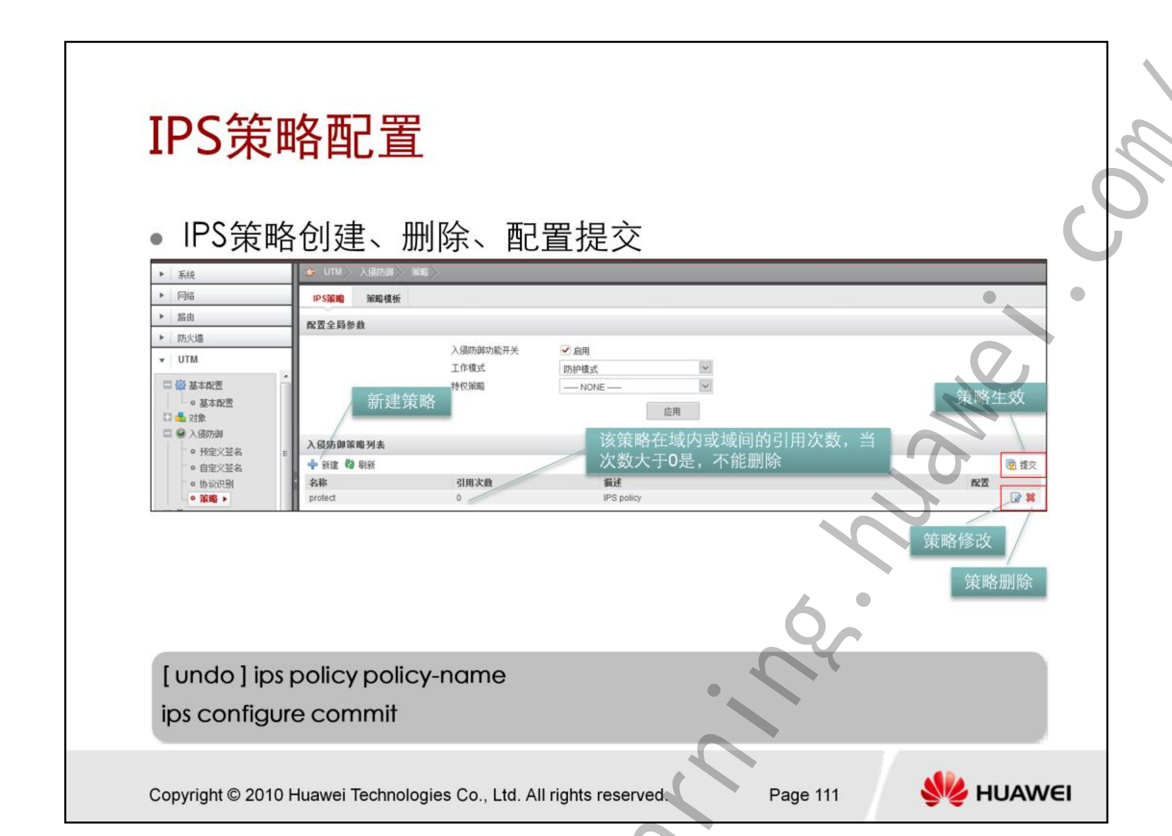
USG5000支持多种常用应用层协议的识别，并提供查询协议识别结果的功能。

IPS全局查询配置

- IPS全局查询、配置




```
display ips global-configuration
ips enable
ips mode { acitive | passive }
Ips policy policy-name privilege
```



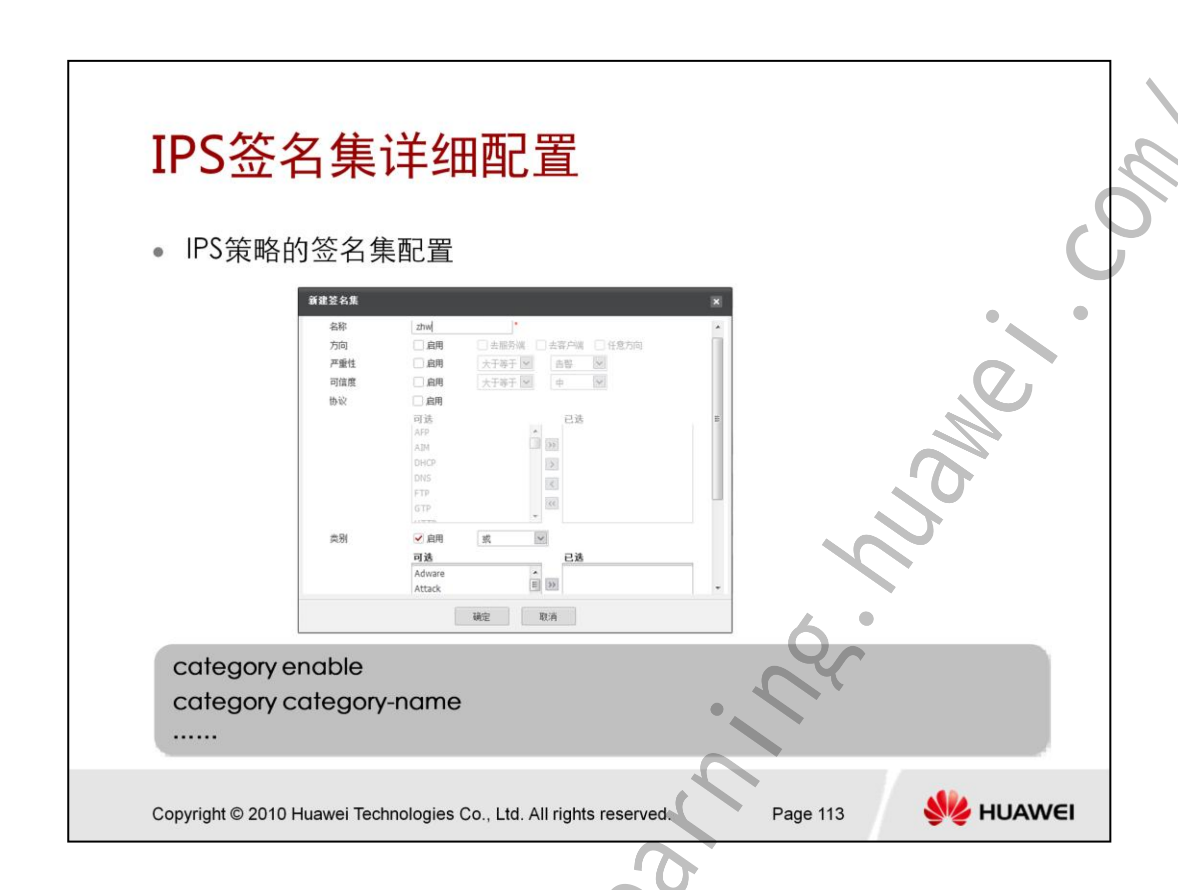
注意：对策略进行操作后，一定要执行 提交 按钮才能生效。因“提交”比较耗时，最好所有修改都完成后再执行。

IPS签名集、覆盖签名配置

- IPS策略的签名集、覆盖签名配置



HUAWEI



当所有选项都没有“开启”时，表示该签名集包含了所有签名。

当有选项开启了但没有指定具体的值，则该签名集不包任何签名。如下图：

方向	☑ 启用	☐ 去服务端	☐ 去客户端	☐ 任意方向

IPS签名集优先级的调整

- 同一个策略下的签名集是有优先级的，当一条签名同时属于该策略下的两个签名集时，该策略的属性为前一个签名集的属性；
- 签名集的优先级可调整，调整后要记得执行“提交”按钮。





IPS覆盖签名详细配置

- IPS策略的覆盖签名查询配置



signature-set signature-set-name
override-signature sig-id

- 覆盖签名的优先集高于签名集中的签名。
- 若覆盖签名中引用过自定义签名，当修改过该自定义签名时，需要在策略页面点击  按钮。

IPS策略模板查询配置

- IPS策略模板信息查询



display ips policy-template { ids | default | all }



总结

- 入侵检测及防御基础知识
- 入侵检测及防御技术原理
- NIP产品安装配置方法
- UTM产品IPS功能配置操作



思考题

- 判断题
  1. 病毒属于入侵行为。
- 多选题
  1. 下列属于基于主机的入侵检测系统（HIDS）特点的是?

A、通过监视和分析主机的审计记录和日志文件来检测入侵;

B、主要用于实时监控网络关键路径的信息，侦听网络上的所有分组，采集数据，分析可疑对象;

C、可监测系统、事件、Win NT下的安全记录以及Unix环境下的系统记录，从中发现可疑行为;

D、侦听主机的端口的活动，并在特定端口被访问时向管理员报警。



习题与答案:

1、病毒属于入侵行为。

答案：错误

2、下列属于基于主机的入侵检测系统（HIDS）特点的是?

A、通过监视和分析主机的审计记录和日志文件来检测入侵;

B、主要用于实时监控网络关键路径的信息，侦听网络上的所有分组，采集数据，分析可疑对象;

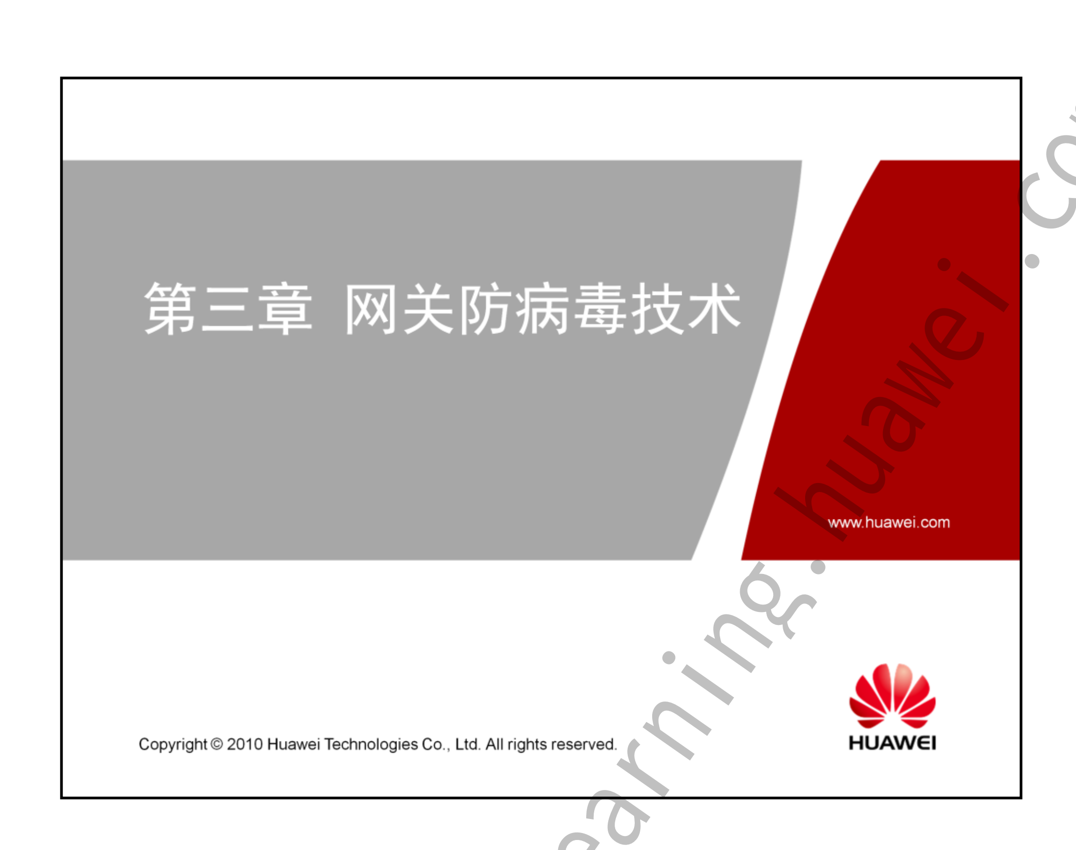
C、可监测系统、事件、Win NT下的安全记录以及Unix环境下的系统记录，从中发现可疑行为;

D、侦听主机的端口的活动，并在特定端口被访问时向管理员报警;

答案：A|C|D

Thank you

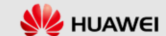
www.huawei.com


第三章 网关防病毒技术
www.huawei.com
HUAWEI



目标

- 学完本课程后，您将能够:
  - 了解计算机病毒基础知识;
  - 掌握病毒特征及常用检测工具;
  - 掌握网关防病毒主要技术;
  - 掌握网关防病毒技术应用。





目录





计算机病毒基本概念

- 计算机病毒
  - 编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码被称为计算机病毒（Computer Virus）。
- 恶意代码
  - 一种程序，它通过把代码在不被察觉的情况下镶嵌到另一段程序中，从而达到破坏被感染电脑数据、运行具有入侵性或破坏性的程序、破坏被感染电脑数据的安全性和完整性的目的。



计算机病毒具有破坏性，复制性和传染性。

木马、间谍软件、蠕虫、逻辑炸弹、漏洞利用程序、垃圾邮件发送器、下载器、拨号器、泛洪攻击器、击键记录器均属于恶意代码。

严格意义上讲计算机病毒是恶意代码的一种，但业界习惯用计算机病毒来指学术上的恶意代码 。

计算机病毒的分类

- 按照恶意代码功能分类：蠕虫、木马；
- 按照传播机制分类：可移动媒体、网络共享、网络扫描、电子邮件、P2P网络；
- 按照感染对象分类：操作系统、应用程序、设备；
- 按照携带者对象分类：可执行文件、脚本、宏、引导区；

 Page 5 

恶意代码的分类方法有很多种。因此，同一种恶意代码可能有多种不同的分法。

- 按照恶意代码功能分类
  - 病毒，属于恶意代码，是附着于程序或文件中的一段计算机代码，以自我复制为明确目的 ，它可能损坏硬件、软件和信息。计算机病毒是蓄意设计的软件程序，它往往寄生于计算机的文件中，目的是干扰计算机操作，记录、毁坏或删除数据，或者自行传播到其他计算机和整个Internet，通常会减慢处理速度并在过程中造成其他问题；
  - 蠕虫，蠕虫是一种通过网络传播的恶性病毒，它具有病毒的一些共性，如传播性、隐蔽性、破坏性等等，同时具有自己的一些特征，如不利用文件寄生（有的只存在于内存中），对网络造成拒绝服务，以及和黑客技术相结合，等等；
  - 木马，特洛伊木马不被认为是计算机病毒或蠕虫，因为它不自行传播。但是，病毒或蠕虫可用于将特洛伊木马作为攻击负载的一部分复制到目标系统上，此过程称为"发送"。特洛伊木马的通常意图是中断用户的工作或系统的正常运行。例如，特洛伊木马可能在系统中提供后门，使黑客可以窃取数据或更改配置设置。
- 按照传播机制分类
  - 可移动媒体：恶意软件最初的、使用最多的传播方式
  - 网络共享：可以复制到大量与网络连接的计算机上



病毒是一种基于硬件和操作系统的程序，具有感染和破坏能力，这与病毒程序的结构有关。

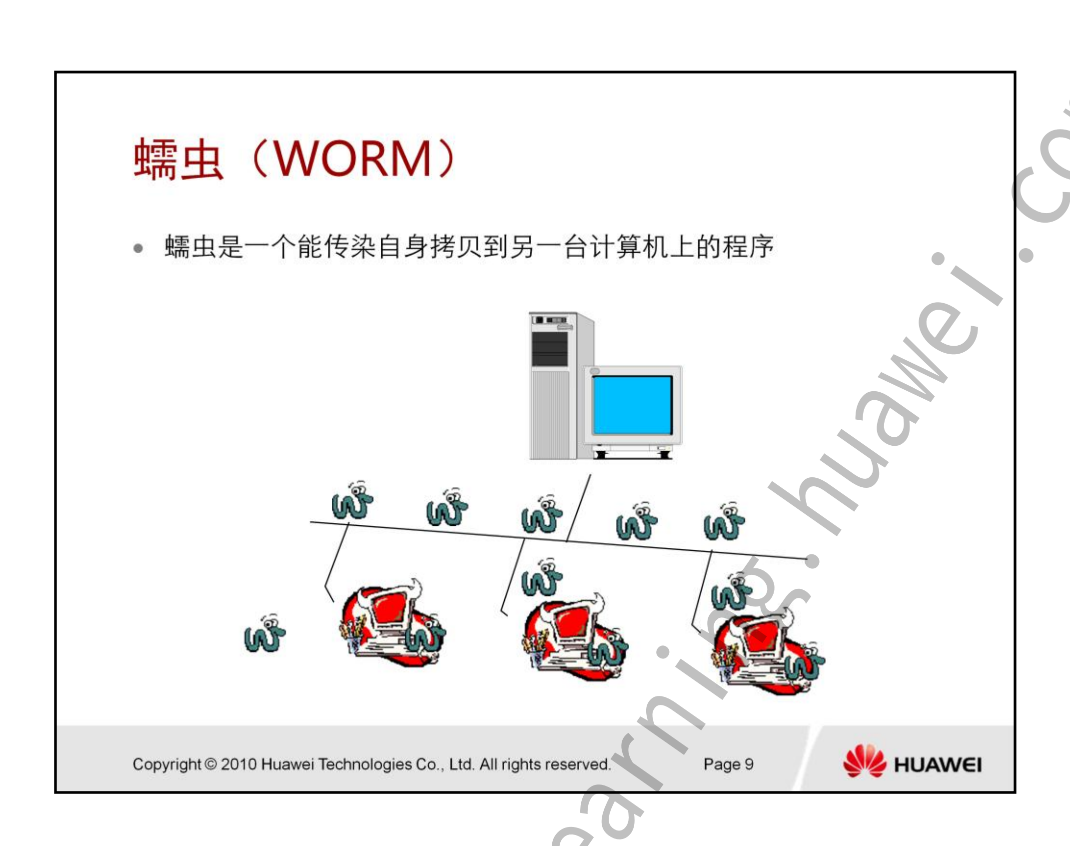
病毒攻击的宿主程序是病毒的栖身地,它是病毒传播的目的地,又是下一次感染的出发点

病毒感染目标可归纳如下：硬盘系统分配表扇区(主引导区)、硬盘引导扇区、软盘引导扇区、可执行文件(.exe)、命令文件(.com)、覆盖文件(.ovl)、COMMAND文件、IBMBIO文件、IBMDOS文件。

病毒感染的过程

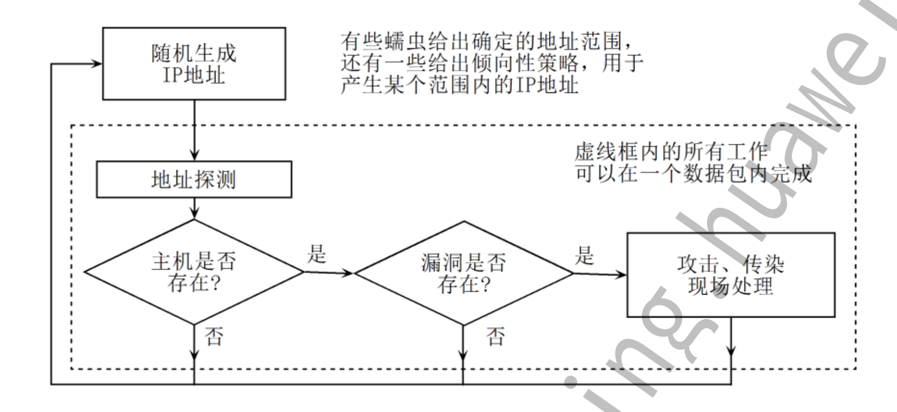
- 计算机病毒感染的一般过程为：
  - 当计算机运行染毒的宿主程序时，病毒夺取控制权；
  - 寻找感染的突破口；
  - 将病毒程序嵌入感染目标中。

计算机病毒的感染过程与生物学病毒的感染过程非常相似，它寄生在宿主程序中，进入计算机并借助操作系统和宿主程序的运行，复制自身、大量繁殖。


蠕虫（WORM）
蠕虫是一个能传染自身拷贝到另一台计算机上的程序
Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.
Page 9
HUAWEI

蠕虫的工作方式

- 蠕虫的工作方式一般是“扫描→攻击→复制”

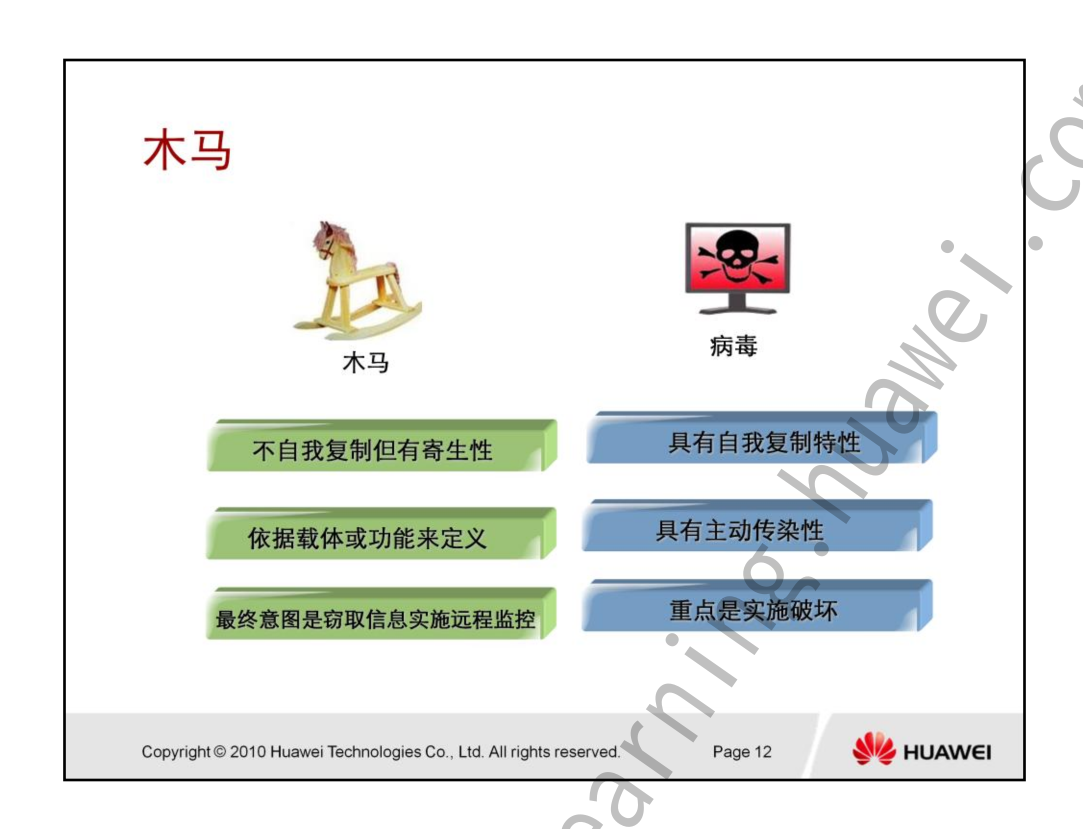




蠕虫与病毒之间区别及联系

项目	病　毒	蠕　虫
存在形式	寄生	独立个体
复制机制	插入到宿主程序(文件)中	自身的拷贝
传染机制	宿主程序运行	系统存在漏洞(Vulnerability)
搜索机制(传染目标)	主要是针对本地文件	针对网络上其它计算机
触发传染	计算机使用者	程序自身
影响重点	文件系统	网络性能、系统性能
计算机使用者角色	病毒传播中的关键环节	无关
防治措施	从宿主程序中摘除	为系统打补丁(Patch)





一般情况下，病毒是依据其能够进行自我复制即传染性的特点而定义的；

特洛伊木马主要根据它的有效载体，或者其功能来定义，更多情况下是根据其意图来定义的；

木马一般不进行自我复制，但具有寄生性，如捆绑在合法程序中得到安装、启动木马的权限，DLL木马甚至采用动态嵌入技术寄生在合法程序的进程中；

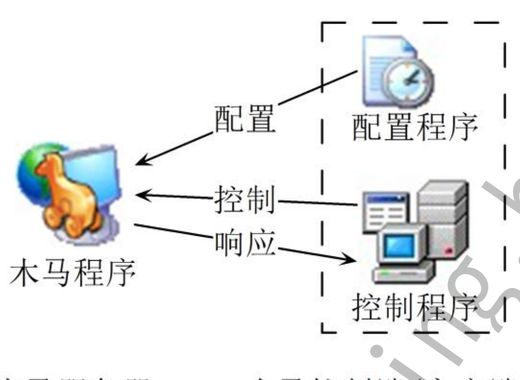
木马一般不具有普通病毒所具有的自我繁殖、主动感染传播等特性，但习惯上将其纳入广义病毒，也就是说，木马也是广义病毒的一个子类；

木马与合法远程控制软件(如pcAnyWhere)的主要区别在于是否具有隐蔽性、是否具有非授权性。

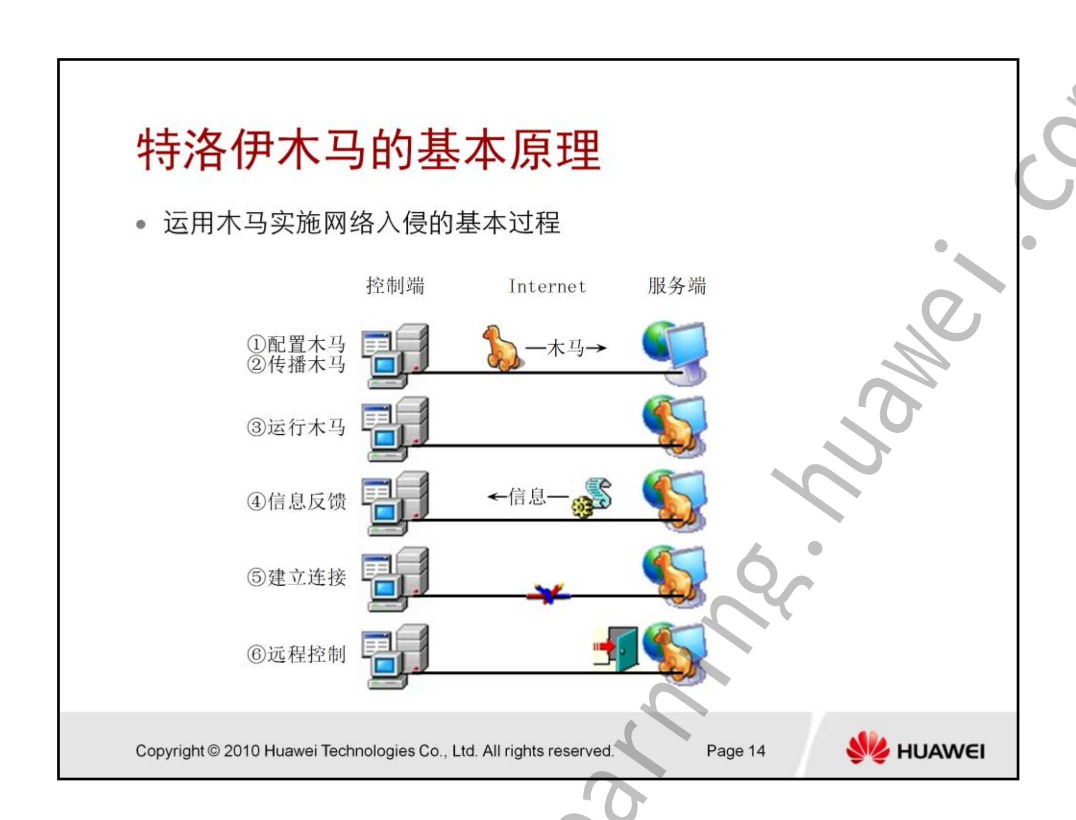


特洛伊木马的结构

- 木马系统软件一般由木马配置程序、控制程序和木马程序(服务器程序)三部分组成







- 传播过程:
  - 黑客利用木马配置工具,生成一个木马的服务端;
  - 通过各种手段(如Spam, Phish, Worm等)安装到用户终端;
  - 利用社会工程学,或者其它技术手段使得木马运行;
  - 木马窃取用户隐私信息发送给黑客;
  - 同时允许黑客控制用户终端。



目录

1. 计算机病毒基础知识
2. **病毒特征及常用检测工具介绍**
3. 网关防病毒技术介绍
4. 网关防病毒技术应用





病毒感染系统后，无疑会对系统做出各种修改和破坏。有时病毒会使受感染的系统出现自动弹出网页、占用高CPU资源、自动弹出/关闭窗口、自动终止某些进程等各种不正常现象。



- 下载特性

很多木马、后门程序间谍软件会自动连接到Internet某Web站点，下载其他的病毒文件或该病毒自身的更新版本/其他变种。

- 后门特性

后门程序及很多木马、蠕虫和间谍软件会在受感染的系统中开启 并侦听某个端口，允许远程恶意用户来对该系统进行远程操控；

某些情况下，病毒还会自动连接到某IRC站点某频道中，使得该频道中特定的恶意用户远程访问受感染的计算机。

一种利用IE控件的下载器病毒示例：

通过Process Explorer发现有一个Internet Explorer进程，但是计算机并没有开启IE程序，并且计算机中没有合法程序中包含IE控件，则计算机中有可能存在下载器病毒。



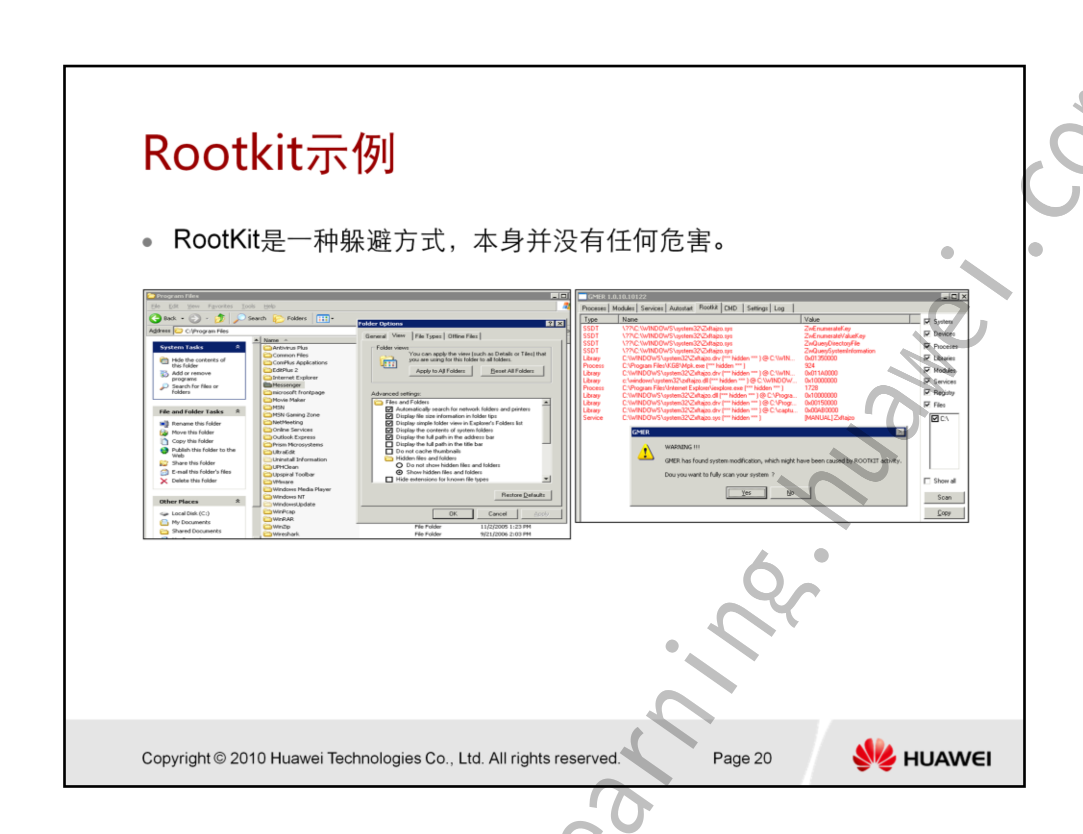
大多数间谍软件和一些木马都会收集系统中用户的私人信息，特别是各种帐号和密码。收集到的信息通常都会被病毒通过自带的SMTP引擎发送到指定的某个指定的邮箱。

自身隐藏特性-Hide&Rootkit

- 自身隐藏特性
  - 多数病毒会将自身文件设置为“隐藏”、“系统”和“只读”属 性，更有一些病毒会通过修改注册表来实现对系统的文件夹访问 权限、显示权限等进行修改，以使其更加隐蔽不易被发现。
- RootKit技术
  - 是一种躲避方式，该技术采用接管底层API的方式使得用户无法通过资源管理器等常规方式查看病毒文件、可疑的套接字等系统信息。

 Page 19 

有一些病毒会使用Rootkit技术来隐藏自身的进程和文件，使得用户更难以发现。使用Rootkit技术的病毒，通常都会有一个.SYS文件加载在系统的驱动中，用以实现Rootkit技术的隐藏功能。



看上图（左），用户无法在资源管理器中看到KGB文件夹，甚至将系统设置为显示任何隐藏文件，还是无法看到KGB这个文件夹，但是通过专业RootKit查看工具GMER或者IceSword却能看到这个文件夹存在，则说明该计算机中存在RootKit利用。

文件感染特性-Infector

- 文件感染特性
  - 文件型病毒的一个特性是感染系统中部分/所有的可执行文件；
  - 病毒会将恶意代码插入到系统中正常的可执行文件中，使得系统 正常文件被破坏而无法运行，或使系统正常文件感染病毒而成为 病毒体；
  - 有的文件型病毒会感染系统中其他类型的文件。



网络攻击特性–Attacker

- 网络攻击
  - 蠕虫病毒会针对微软操作系统或其他程序存在的漏洞进行攻击，从而导致受攻击的计算机出现各种异常现象，或是通过漏洞在受攻击的计算机上远程执行恶意代码。
  - 木马和蠕虫病毒会修改计算机的网络设置，使该计算机无法访问网络。
  - 木马和蠕虫还会向网络中其他计算机攻击、发送大量数据包以阻塞网络，甚至通过散布虚假网关地址的广播包来欺骗网络中其他计算机，从而使得整个网络瘫痪。



常见病毒传播途径—电子邮件

- HTML正文可能被嵌入恶意脚本；
- 邮件附件携带病毒压缩文件；
- 利用社会工程学进行伪装，增大病毒传播机会；
- 快捷传播特性。





常见病毒传播途径—网络共享

- 病毒会搜索本地网络中存在的共享，包括默认共享，如ADMIN$ ，IPC$,E$,D$,C$；
- 通过空口令或弱口令猜测，获得完全访问权限；
- 病毒自带口令猜测列表；
- 将自身复制到网络共享文件夹中；
- 通常以游戏,CDKEY等相关名字命名。







常见病毒传播途径—P2P共享软件

- 将自身复制到P2P共享文件夹；
- 通常以游戏,CDKEY等相关名字命名；
- 通过P2P软件共享给网络用户；
- 利用社会工程学进行伪装，诱使用户下载。







常见病毒传播途径—系统漏洞

- 由于操作系统固有的一些设计缺陷,导致被恶意用户通过畸形的方式利用后,可执行任意代码,这就是系统漏洞。
- 病毒往往利用系统漏洞进入系统，达到传播的目的。
- 一些大家熟知的漏洞：
  - RPC-DCOM 缓冲区溢出 (MS03-026) 冲击波；
  - LSASS (MS04-011) 震荡波。



常见病毒传播途径—广告软件/灰色软件

- 由于广告软件/灰色软件的定义，它们有时候是由用户主动安装，更多的是与其他正常软件进行绑定。

☑ UltraEdit （必须）
☑ 安装 UltraCompare Pro 3.00a （可选）
☑ 安装 UEHelper 1.1.1 （可选）
☑ 创建开始菜单组 （可选）
☑ 创建快捷启动栏图标 （可选）
☑ 创建桌面图标 （可选）
☑ 安装 CNNIC 中文上网 （可选）



常见病毒传播途径—其他

- 网页感染；
- 与正常软件捆绑；
- 用户直接运行病毒程序；
- 由其他恶意程序释放。

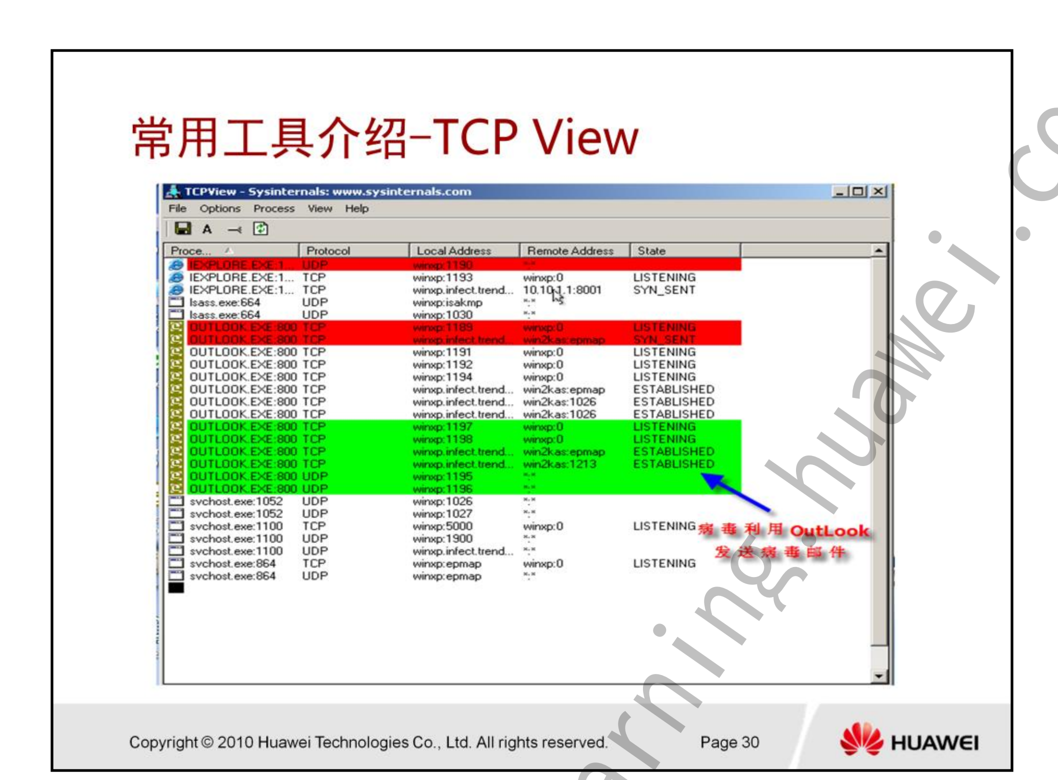
  HUAWEI

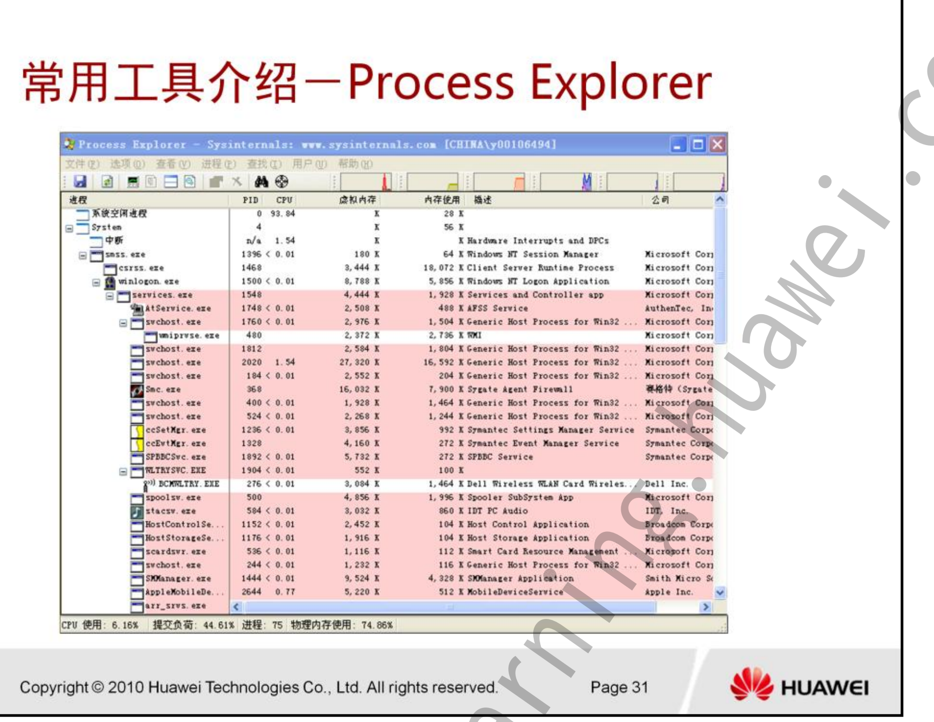
目前大多数的木马、间谍软件等病毒都是通过这几种方式进入系统。它们通常都不具备传播性。

常用工具介绍-TCP View

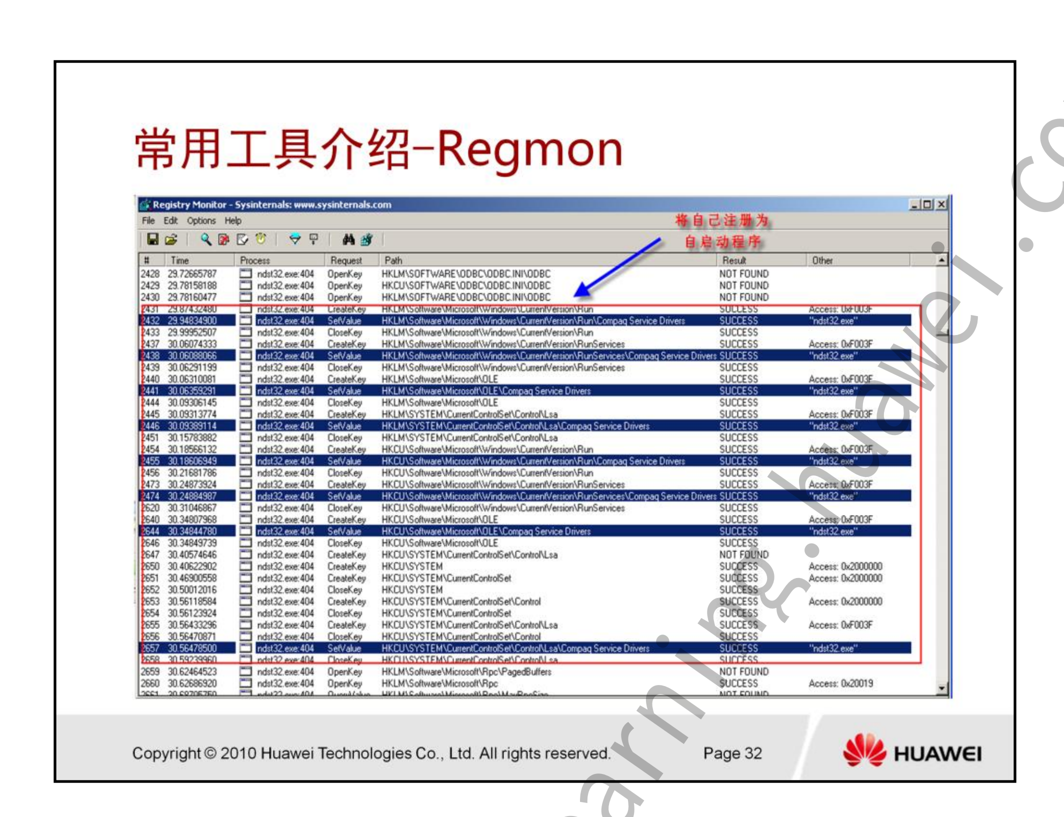
- TCP View 功能
  - 查看系统的网络连接信息(远程地址,协议,端口号);
  - 查看系统的网络连接状况(发起连接,已连接,已断开);
  - 查看进程打开的端口;
  - 动态刷新列表;
  - 多用于查看 蠕虫,后门,间谍等恶意程序。



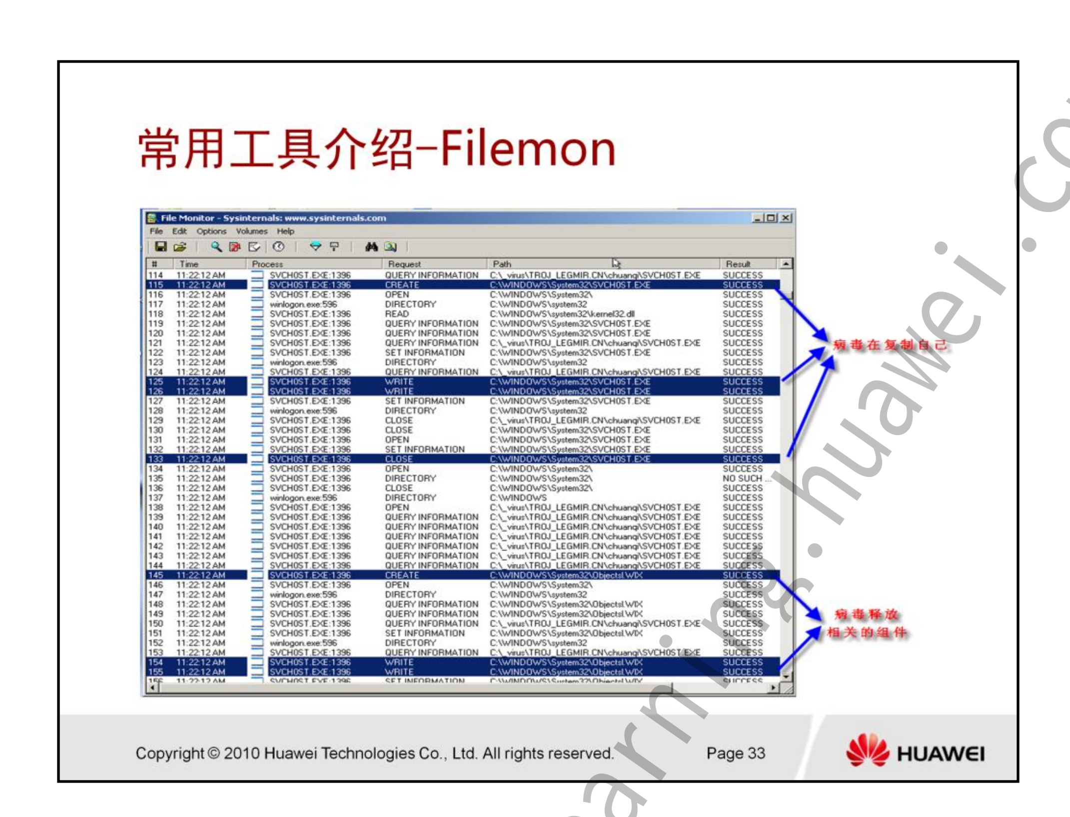

常用工具介绍-TCP View
TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Proce... Protocol Local Address Remote Address State
IEXPLORE.EXE:1... TCP winxp:1193 winxp:0 LISTENING
IEXPLORE.EXE:1... TCP winxp.infect.trend... 10.10.1.1:8001 SYN_SENT
lsass.exe:664 UDP winxp:isakmp
lsass.exe:664 UDP winxp:1030
OUTLOOK.EXE:800 TCP winxp:1191 winxp:0 LISTENING
OUTLOOK.EXE:800 TCP winxp:1192 winxp:0 LISTENING
OUTLOOK.EXE:800 TCP winxp:1194 winxp:0 LISTENING
OUTLOOK.EXE:800 TCP winxp.infect.trend... win2kas:epmap ESTABLISHED
OUTLOOK.EXE:800 TCP winxp.infect.trend... win2kas:1026 ESTABLISHED
OUTLOOK.EXE:800 TCP winxp.infect.trend... win2kas:1026 ESTABLISHED
svchost.exe:1052 UDP winxp:1026
svchost.exe:1052 UDP winxp:1027
svchost.exe:1100 TCP winxp:5000 winxp:0 LISTENING
svchost.exe:1100 UDP winxp:1900
svchost.exe:1100 UDP winxp.infect.trend...
svchost.exe:864 TCP winxp:epmap winxp:0 LISTENING
svchost.exe:864 UDP winxp:epmap
病毒利用OutLook
发送病毒邮件
Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.
Page 30
HUAWEI



- Process Explorer功能
  - 显示被执行的映像文件的完整路径；
  - 显示进程安全令牌；
  - 加亮显示进程和线程列表中的变化；
  - 显示作业中的进程，以及作业的细节；
  - 显示运行.NET/WinFX应用的进程，以及与.NET相关的细节；
  - 显示进程和线程的启动时间;
  - 显示内存映射文件的完整列表；
  - 能够挂起一个进程 或杀死一个线程。



- Regmon主要功能
  - 监视系统中注册表的操作；
  - 如 注册表的打开,写入,读取,查询,删除,编辑等；
  - 多用于监视病毒的自启动信息和方式。



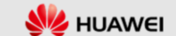
- Filemon主要功能
  - 监视文件系统的操作;
  - 如建立文件,打开文件,写文件;
  - 读文件,查询文件信息等;
  - 多用于查找Dropper的主体程序。



- 进程管理
  - 显示隐藏进程；
  - 杀除普通方式无法杀除的进程。
- 注册表管理
  - 显示隐藏注册表项；
  - 修改普通方式无法修改的注册表项。
- 文件管理
  - 显示隐藏文件；
  - 删除普通方式无法删除的文件。



目录



网关防病毒主要实现方式

- 基于代理的反病毒网关：
- 基于流扫描的反病毒网关：

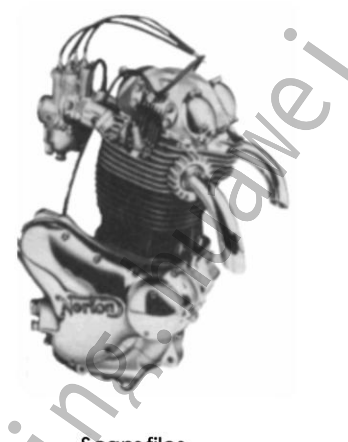


目前设备厂商（包括UTM、AVG）的AV扫描方式，分为两种：流扫描方式和代理扫描方式。

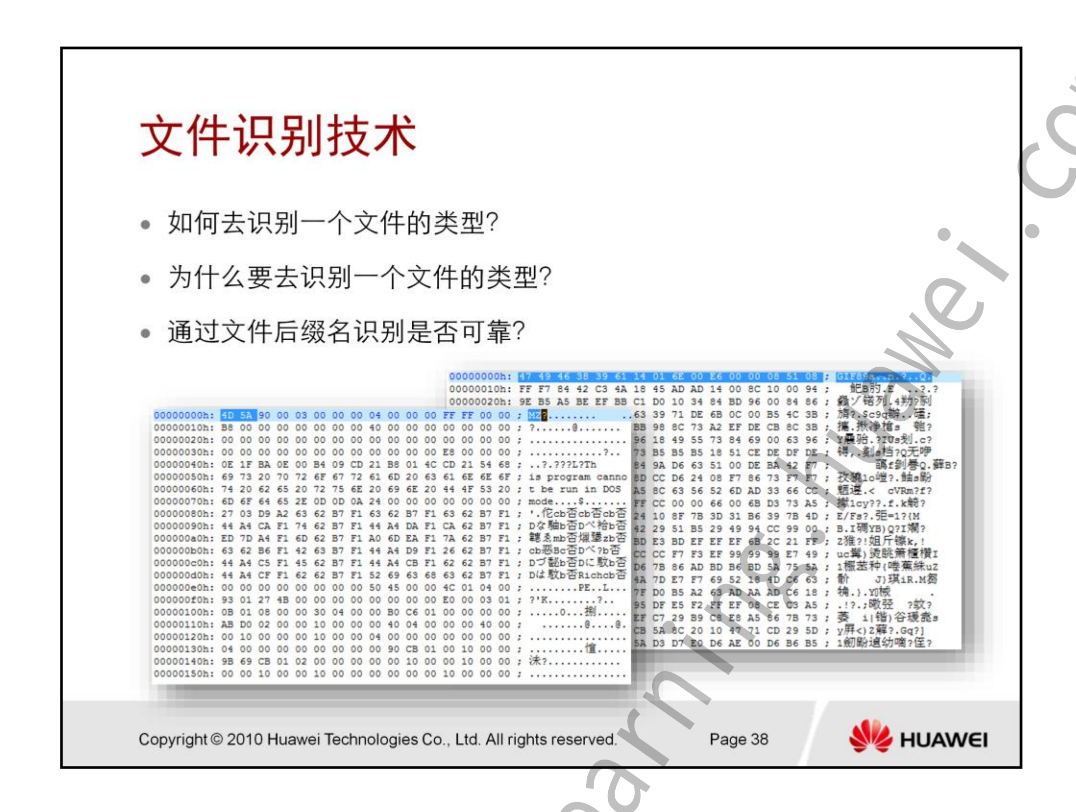
- 基于代理的反病毒网关：
  - 实现原理：将所有经过网关的需要进行病毒检测的数据报文透明的转交给网关自身的协议栈，通过网关自身的协议栈将文件全部缓存下来后， 再送入病毒检测引擎进行病毒检测；
  - 优缺点：可以进行更多如解压，脱壳等高级操作，检测率高，但是，由于进行了文件全缓存，其性能、系统开销将会比较大。
- 基于流扫描的反病毒网关：
  - 工作原理：依赖于状态检测技术以及协议解析技术，简单的提取文件的特征与本地签名库进行匹配；
  - 优缺点：性能高，开销小，但该方式检测率有限，无法应对加壳、压缩等方式处理过的文件。

反病毒引擎的典型技术

- 文件识别技术
- 脱壳技术
- 解压技术
- 静态识别技术
- 动态虚拟机技术







识别一个文件的类型，可以使得我们反病毒技术更加准确可靠，如：一般的病毒很可能的存在于PE文件中（PE文件是Windows系统中的可执行文件，如EXE文件就是PE文件中的一种）。

识别一个文件的类型有多种方式：根据后缀名和根据文件的真实内容。

后缀名是允许用户修改的，所以不可靠，根据文件真实内容识别更加可靠，文件真实类型的识别一般可以由文件的前64字节就可以判断出。



恶意代码为了隐藏自己通常会加壳。

为了使病毒检测引擎能够检测出恶意代码中的特征，病毒检测引擎不得不进行脱壳工作。

脱壳分为硬脱壳和动态脱壳，硬脱壳，这是指找出加壳软件的加壳算法，写出逆向算法，就像压缩和解压缩一样。由于加壳的程序运行时必须还原成原始形态，即加壳程序会在运行时自行脱掉 “马甲” 。

解压技术

- 文件压缩出现在网络的各个位置，也许一个HTTP普通网页请求就可能是利用压缩格式将数据传回。
- 对于压缩过的文件无论是入侵检测系统还是病毒检测系统都无法直接检测。





静态识别技术

- 从病毒体内提取的原始数据片断，以及该片断的位置信息。

优点	缺点
• 精确，误报少； • 快速，静态分析。	• 提取自病毒体，滞后于病毒出现； • 抗“特征”变化性有限。



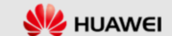
动态虚拟机技术

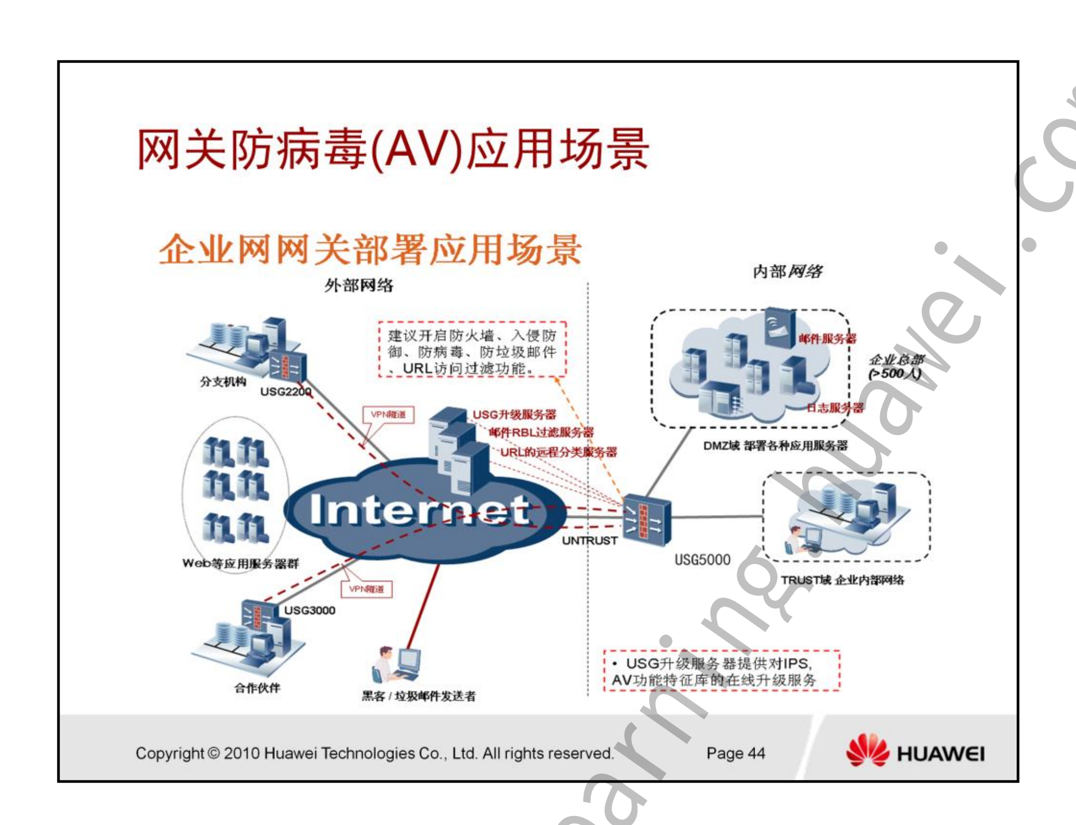
- 虚拟执行的概念
  - 提供一个完全模拟x86指令集的可执行受管理程序的执行环境，能让待检测的程序直接在该环境中执行一些指令。
- 虚拟执行的分类
  - 真实环境的执行
  - 隔离环境的执行
  - 虚拟环境的执行
- 为什么需要虚拟执行
  - 传统的静态分析技术、脱壳技术等反病毒技术已无法应对病毒免杀技术的发展





目录





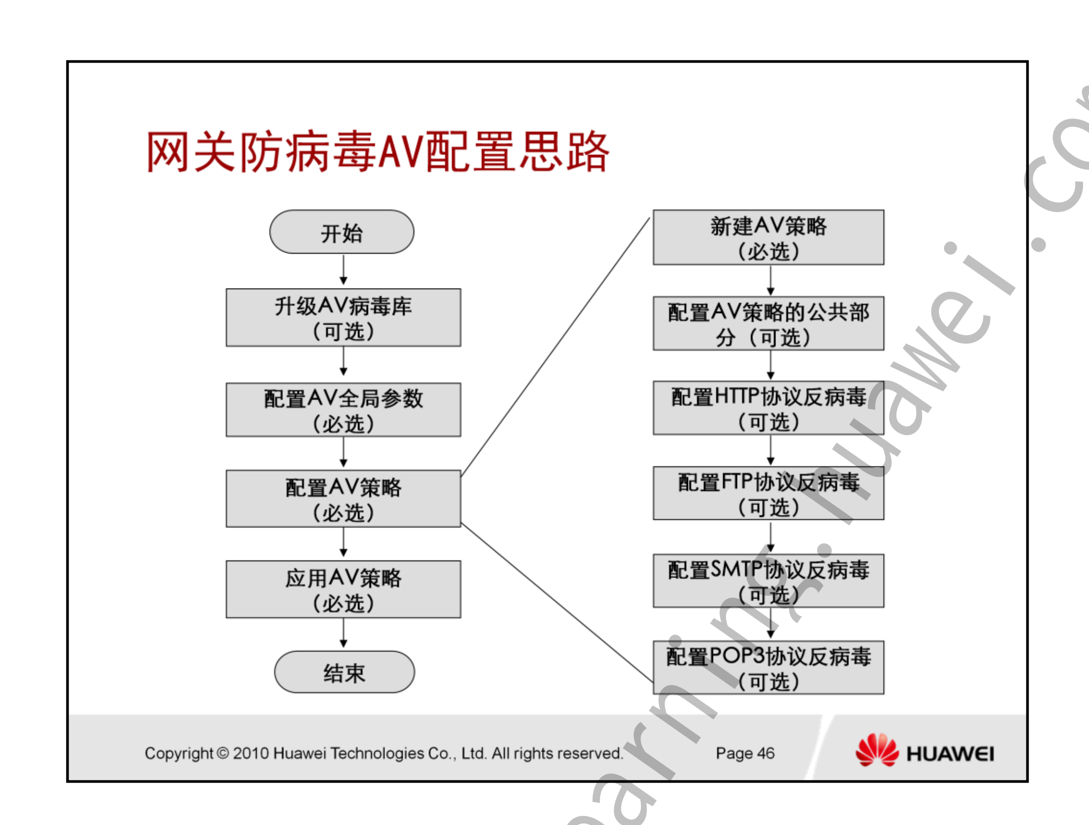
当前，网络安全威胁的性质已发生很大的变化。尽管传统的 L2-4 防火墙仍然是网络安全的必需要素，但以入侵、病毒为代表的新型动态攻击正在引发前所未有的破坏。这些攻击不仅致使传统的防火墙变得毫无用武之地，而且还需不断更新攻击数据库，才能进行有效防护。

USG5000 的UTM特性集成 Symantec 的病毒库和病毒引擎技术，可以保护网络，使其远离多种动态威胁，包括病毒、间谍软件、蠕虫、木马病毒、后门和其它恶意代码等。

网关防病毒AV功能列表

- 支持基于 HTTP/SMTP/POP3 协议的文件病毒扫描
- 支持对压缩加壳病毒的检测
- 支持病毒引擎和病毒库升级
- 支持病毒扫描和协议策略的热备
- 支持透明模式和混合模式下的病毒扫描
- 支持功能/升级年限的license 控制





- 配置垃圾邮件过滤全局参数

　　当需要在邮件过滤策略中引用垃圾邮件过滤时需要配置，内容包括：　垃圾邮件过滤功能全局开关、本地黑白名单使能开关、查询垃圾邮件服务器的DNS地址。

- 创建本地黑白名单

　　当需要在垃圾邮件过滤中使用本地黑名单时需要配置。

- 配置预定义策略

　　如果需要使用系统预置的Symantec服务器作为RBL服务器进行RBL远程查询，需要配置预定义策略。

- 配置自定义策略

　　如果需要使用自定义的服务器作为RBL服务器进行RBL远程查询，请配置自定义策略。

配置AV全局参数

UTM > 反病毒 > 策略

配置全局参数

AV功能	①	☑ 启用
扫描等级		中
最大解压层数		10 <2-20>层
安全改善计划		☑ 启用

参与安全改善计划后，设备可以在线收集您所在的网络的安全性问题，包括病毒以及攻击的信息，这些信息将发送给Huawei安全服务中心，以帮助我们更好的保护您的网络。

② 应用

- 启用/禁用全局病毒扫描功能。
- 配置全局病毒扫描的等级。
- 配置全局病毒扫描的最大解压层数。
- 启用/禁用安全改善计划功能。

  HUAWEI

- 启用/禁用全局病毒扫描功能

只有启用了AV功能，应用在域间的AV策略才生效。AV功能开关只对新建连接生效，对启用AV功能之前已存在的连接不生效。

- 配置全局病毒扫描的等级

扫描等级共有3级，默认为2级(中)。等级越高对文件的扫描深度越深，系统消耗的资源也越多。扫描等级取值越高，病毒检测率会越高，但产生误报的可能性也越大。改变扫描等级会导致AV引擎重新初始化。

- 配置全局病毒扫描的最大解压层数

出于系统资源的考虑，超大压缩层数的设置也可以根据用户的网络现状设置，文件嵌套超过10层为压缩层数超限。

当网络上传输的文件的压缩层数小于或等于最大解压层数时，文件将被解压，然后进行扫描；当文件的压缩层数大于最大解压层数时，不对文件进行扫描，并按照超过最大解压层数的动作处理。

当经过设备的文件压缩层数大于最大解压层数时，设备根据AV策略公共配置的“超解压层数文件”中的处理方式丢弃或放行该文件。

- 启用/禁用安全改善计划功能

启用该功能后，设备可以在线收集您所在的网络的安全性问题，包括病毒和攻击信息，并将这些信息发送给安全服务中心，以帮助我们更好的保护您的网络。

配置AV全局参数

UTM > 反病毒 > 策略

配置全局参数

AV功能 ☑ 启用

扫描等级 中

最大解压层数 10 <2-20>层

安全改善计划 ☑ 启用

参与安全改善计划后，设备可以在线收集您所在的网络的安全性问题，包括病毒以及攻击的信息，这些信息将发送给Huawei安全服务中心，以帮助我们更好的保护您的网络。

应用

① AV策略列表

新建 删除 刷新

名称	引用次数	描述	HTTP协议	FTP协议	SMTP协议	POP3协议	② 配置
mytest	0	Anti-Virus policy					

新建AV策略

名称 ③ abc *

描述 Anti-Virus policy

④ 应用 返回

- 配置AV全局参数
  - 选择“UTM > 反病毒 > 策略”。
  - 在“配置全局参数”区域框中配置AV全局参数。
  - 单击“应用”。

  AV全局参数的配置对所有AV策略都有效。
- 新建AV策略
  - 选择“UTM > 反病毒 > 策略”。
  - 单击“新建”。
  - 输入新建AV策略的名称和描述。
  - 单击“应用”。

配置AV策略的公共部分

公共配置			
超大文件 ①	允许	密码保护文件 ②	允许
受损文件	允许	超解压层数文件	允许

- 超大文件
- 密码保护文件
- 受损文件
- 超解压层数文件

HUAWEI

- 在“公共配置”区域框中配置参数。（超大文件、密码保护文件、受损文件、超解压层数文件）
  - 允许：允许文件通过，对HTTP、FTP协议传输的文件：允许文件通过，只产生日志；对SMTP、POP3协议传输的文件：允许文件通过，同时在邮件正文中添加宣告并产生日志。
  - 拒绝：阻断文件通过，对HTTP、FTP协议传输的文件：阻断文件通过，同时向客户端推送Web页面并产生日志；对SMTP、POP3协议传输的文件：阻断邮件的附件，同时在邮件正文中添加宣告并产生日志。
  - 单击“应用”，完成公共配置。

AV策略的公共部分对该策略的所有协议都有效。

出于系统资源的考虑，超大文件和超大压缩层数的文件，用户的配置通过还是阻断。对于密码保护的文件，由于网关设备不具备密码破解能力，因此可以由用户设定对密码保护文件的处理方式为通过还是阻断。

文件在主机上以一定的格式保存、读取和解析，对于格式损坏的文件，设备可以直接检测到，并根据用户的配置允许通过或阻断。

配置HTTP协议反病毒

- 对使用HTTP协议传输的文件启用病毒扫描。
- 配置对HTTP文件进行病毒扫描的参数
- 配置响应方式及推送内容

  HUAWEI

- 在“HTTP协议配置”区域框中配置各参数。
  - 启用病毒扫描
  - HTTP传输模式
  - 断点续传
  - 传输体验，启用此功能可提高文件传输速率，但有可能导致带病毒的文件漏阻断。在观看在线视频的情况下，请启用传输体验。
  - 文件大小上限。以post方式上传多个文件时，设备将根据多个文件的总大小判定是否为超大文件；当经过设备的HTTP协议文件大于最大扫描文件大小的值时，设备根据公共配置中超大文件的处理方式丢弃或放行该文件。
  - 文件扫描方式，智能扫描：根据文件的真实类型进行扫描。此方式下设备扫描所有文件；指定扩展名扫描：根据文件扩展名表示的文件类型进行扫描。
  - 响应方式，告警：设备只产生日志，不对HTTP协议传输的文件进行处理就发送出去；阻断：设备断开与HTTP服务器的连接并阻断文件，向客户端推送Web页面并产生日志
  - Web推送内容，当设备阻断文件传输时向客户端推送的Web页面内容。

配置FTP协议反病毒

FTP协议配置

病毒扫描	①	☑ 启用	
FTP传输模式	②	☑ 上传	☑ 下载
断点续传		☑ 启用	
传输体验		☐ 启用	
文件大小上限		1 <1-20>MB	
文件扫描方式		○ 智能扫描	◉ 指定扩展名扫描　配置
响应方式	③	告警	
推送内容		The uploaded or downloaded file has security risks	

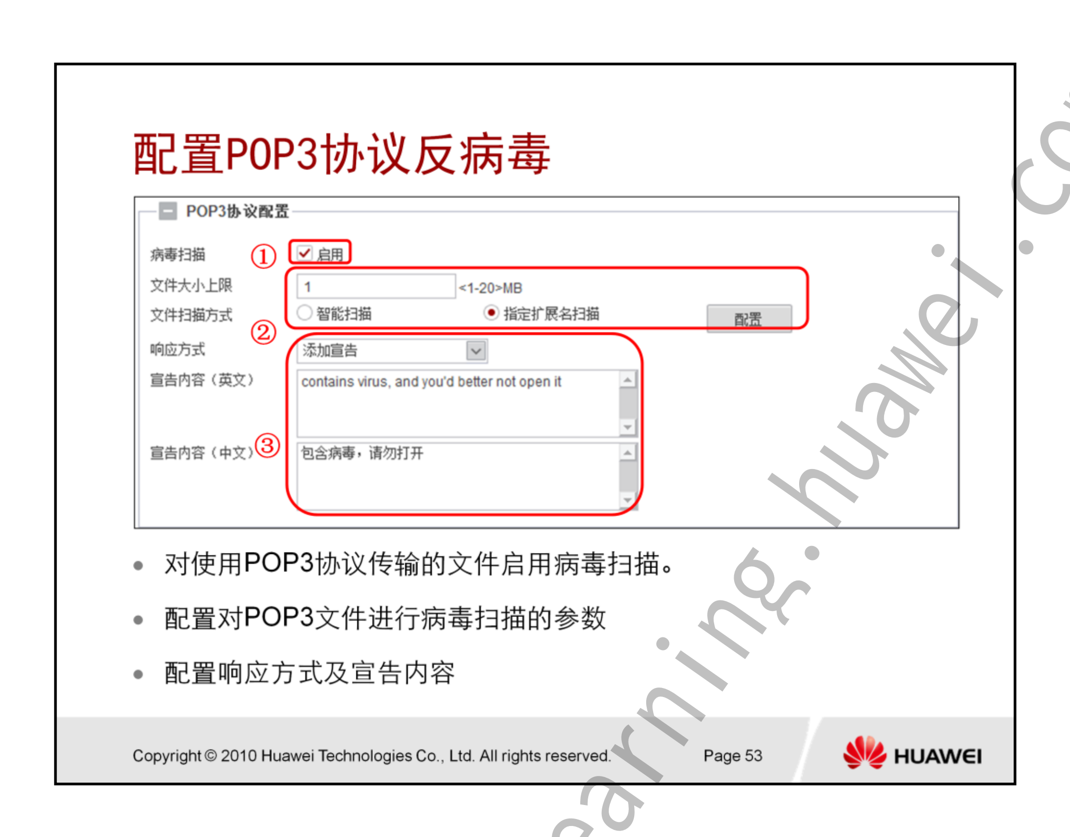
- 对使用FTP协议传输的文件启用病毒扫描。
- 配置对FTP文件进行病毒扫描的参数
- 配置响应方式及推送内容

HUAWEI

- 在“FTP协议配置”区域框中配置各参数。
  - 启用病毒扫描
  - FTP传输模式
  - 断点续传
  - 传输体验，启用此功能可提高文件传输速率，但有可能导致带病毒的文件漏阻断。在观看在线视频的情况下，请启用传输体验。
  - 文件大小上限，当经过设备的FTP协议文件大于最大扫描文件大小的值时，设备根据公共配置中超大文件的处理方式丢弃或放行该文件。
  - 文件扫描方式，智能扫描：根据文件的真实类型进行扫描。此方式下设备扫描所有文件。 指定扩展名扫描：根据文件扩展名表示的文件类型进行扫描。
  - 响应方式，告警：设备只产生日志，不对HTTP协议传输的文件进行处理就发送出去；阻断：设备断开与HTTP服务器的连接并阻断文件，向客户端推送Web页面并产生日志。
  - Web推送内容，当设备阻断文件传输时向客户端推送的Web页面内容。



- 在“SMTP协议配置”区域框中配置各参数。
  - 启用病毒扫描
  - 文件大小上限，当经过设备的SMTP协议文件大于最大扫描文件大小的值时，设备根据公共配置中超大文件的处理方式丢弃或放行该文件。
  - 文件扫描方式，智能扫描：根据文件的真实类型进行扫描。此方式下设备扫描所有文件；指定扩展名扫描：根据文件扩展名表示的文件类型进行扫描。
  - 响应方式，告警：设备只产生日志，不对HTTP协议传输的文件进行处理就发送出去；阻断：设备断开与HTTP服务器的连接并阻断文件，向客户端推送Web页面并产生日志
  - 宣告内容（英文），此模式下配置的宣告内容只会添加到字符集是US-ASCII和UTF-7的邮件中。
  - 宣告内容（中文），此模式下配置的宣告内容只会添加到字符集是GB2312的邮件中。



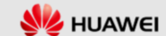
- 在“POP3协议配置”区域框中配置各参数。
  - 启用病毒扫描
  - 文件大小上限，当经过设备的POP3协议文件大于最大扫描文件大小的值时，设备根据公共配置中超大文件的处理方式丢弃或放行该文件。
  - 文件扫描方式，智能扫描：根据文件的真实类型进行扫描。此方式下设备扫描所有文件；指定扩展名扫描：根据文件扩展名表示的文件类型进行扫描。
  - 响应方式，告警：设备只产生日志，不对HTTP协议传输的文件进行处理就发送出去；阻断：设备断开与HTTP服务器的连接并阻断文件，向客户端推送Web页面并产生日志
  - 宣告内容（英文），此模式下配置的宣告内容只会添加到字符集是US-ASCII和UTF-7的邮件中。
  - 宣告内容（中文），此模式下配置的宣告内容只会添加到字符集是GB2312的邮件中。



- 配置完策略后，需要应用邮件过滤策略。
  - 选择“防火墙 > 安全策略 > 转发策略”。
  - 在“转发策略列表”中，单击“新建”。
  - 在“新建转发策略”区域，依次输入或选择各项参数。
  - 选中“AV”复选框，选择前面配置的相应AV策略。
  - 单击“应用”，完成AV防病毒策略应用的配置。

AV典型故障处理

- AV检测失效定位过程
  - 原因一：没有使能AV全局开关
  - 原因二：AV策略配置不当
  - 原因三：未加载AV引擎
  - 原因四：License过期
  - 原因五：内存不足
  - 原因六：AV引擎本身问题



AV典型故障处理

- **原因一：没有使能AV全局开关**
  1. 执行命令display av global-configuration，查看av全局开关使能状态

     Anti-Virus Global Configuration Info

     ```
     ----------------------------------------------------------
     Anti-Virus global switch :          Enable
     Scan level                :            2
     Max decompressable layer :          10
     ----------------------------------------------------------
     ```

     global switch表示av全 局开关的使能状态。
     如果状态为enable，继续执行原因二。
     如果状态为disable，继续执行2。
  2. 在系统视图下执行命令av enable，使能av全局开关；
  3. 检查故障是否消除，如果没有，继续执行原因二。



AV典型故障处理

- 原因二：AV策略配置不当

  1. 执行命令dis policy interzone zone1 zone2 {inbound | outbound}；

  ```
  firewall default packet-filter is permit
  action permit
  policy service service-set ip
  policy source any
  policy destination any
  policy av abc
  ```

  policy av abc表示域间应用了av策略abc。

  如果未应用av策略，继续执行2；否则继续执行原因三。

  2. 创建av策略并应用于域间，具体配置步骤请参见av功能配置；
  3. 检查故障是否消除，如果没有，继续执行原因三。



AV典型故障处理

- 原因三：未加载AV引擎
  1. 执行命令display av version，查看是否已加载AV引擎及签名库；

  Version number : 20090811.001
  Engine version : 1.000
  Engine size : 2008792 bytes
  Signature database version : 20090811.001
  Signature database size : 48057345 bytes
  Update time : 18:41:13 2009/08/11
  Issue time of the update file : 02:32:24 2009/08/12

  如果Current version没有或者该版本不是最新发布版本，继续执行2；否则继续执行原因四。

  2. 对设备av引擎及签名库进行本地升级或者远程升级，具体步骤请参见《USG系列防火墙软件升级指导》。

  3. 检查故障是否消除，如果没有，继续执行原因四。



AV典型故障处理

- **原因四：License过期**

  1.执行命令display license，查看License是否过期。

  [UTM5000_A]display license
  06:33:39 2008/09/16
  Device ESN is: 2102351337Z08C000032
  Have already activated 1 License file,the file is:
  flash:/on1032318.dat   Activated time: 2008/08/13 09:21:08
  VPN   : 7000
  VFW   : 50
  GTP   : ENABLED
  IPS   : ENABLED; Expiration date: 2010-04-15
  URL Filter   : ENABLED; Expiration date: 2008-12-15
  Anti Virus   : ENABLED; Expiration date: 2010-04-15

  如果License过期，请购买License；否则继续执行原因五

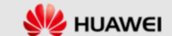


原因五：内存不足、原因六：AV引擎本身的问题请联系厂商工程师解决。



总结

- 恶意代码、病毒、木马基础知识
- 常用病毒检测工具的基础知识
- 网关防病毒主要技术
- 网关防病毒技术的典型应用



思考题

- 判断题

  1. 开启AV功能的断点续传功能后，分块传输不再扫描，直接通过。

- 单选题

  1. AV功能不能支持的协议类型是:

  A、HTTP　B、FTP　C、SMTP　D、POP3

- 多选题

  1. 病毒程序的结构一般由4部分组成:

  A、感染标记　B、感染程序模块 C、破坏程序模块　D、触发程序模块



习题与答案:

1、病毒程序的结构一般由4部分组成:

A、感染标记 B、感染程序模块 C、破坏程序模块 D、触发程序模块

答案：A|B|C|D

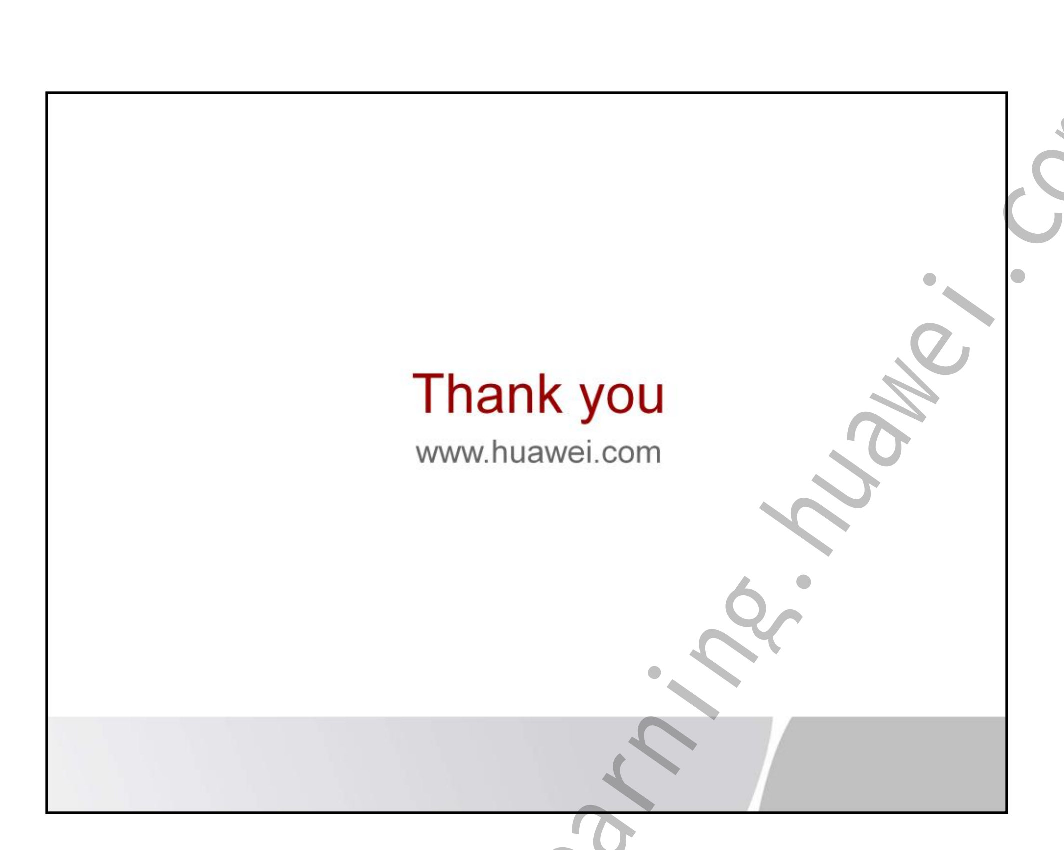
2、AV功能不能支持的协议类型是:

A、HTTP B、FTP C、SMTP D、POP3

答案：B

3、开启AV功能的断点续传功能后，分块传输不再扫描，直接通过。

答案：正确


Thank you
www.huawei.com


第四章 WEB过滤技术
•www.huawei.com
•Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



目标

- 学完本课程后，您将能够:
  - 了解WEB过滤技术基础知识；
  - 了解常见的WEB威胁；
  - 熟悉WEB过滤关键技术；
  - 掌握WEB过滤技术应用。





目录



WEB过滤技术

- WEB过滤技术是一种针对WEB漏洞、WEB分类等进行深度检测然后进行访问控制的安全上网管理技术，包括：
  - URL过滤
  - 搜索关键字过滤
  - 基于WEB内容过滤
  - 恶意网页URL过滤



随着互联网应用的迅速发展，计算机网络在经济和生活的各个领域迅速普及，使得信息的获取、共享和传播更加方便，但同时也给企业带来了前所未有的威胁：员工随意不受控地访问非法网站，不仅严重影响工作效率而且威胁企业网络安全。

URL过滤、搜索关键字过滤、Web内容过滤技术分别从URL、搜索关键字、Web页面等维度控制内网用户的上网行为。

- URL过滤：对用户的HTTP请求进行访问控制，允许或禁止用户访问某些网络资源，可以达到规范上网行为的目的。
- 搜索关键字过滤：指对指定搜索关键字进行过滤，控制内网用户的搜索内容，防止用户获得敏感信息。
- 基于WEB内容过滤：对网页内容进行分析和过滤，比如网页关键字等WEB应用。
- 恶意网页URL过滤：利用恶意网页检测技术分析恶意网页并将恶意网页URL计入分类列表，按预先制定的过滤策略实施控制。

通过Web过滤技术，您可以防止内网用户进行以下操作：访问不合适的网站、查看非法网页内容或在上传/下载不符合要求的文件、通过搜索引擎搜索敏感信息等。

WEB相关威胁及问题

- 僵尸和病毒等威胁
- 账号、密码等机密信息泄漏
- 带宽占用，工作效率降低
- 法律风险



对于企业而言，内部员工过分或不适当的WEB资源访问不仅给企业带来了生产力和网络带宽的损失，还严重威胁着企业的网络安全架构和信息系统，甚至网络上的不适当或非法内容还极大危害着企业员工个人的身心健康甚至给企业带来法律问题。

- 僵尸和病毒等威胁

员工访问WEB 网页时容易被不安全的链接或者恶意下载威胁，终端被植入各种恶意的代码程序，使所在机构终端成为僵尸或者感染病毒。

- 账号、密码等机密信息泄漏

员工访问WEB 网页时容易被含有欺骗信息的钓鱼网站所欺骗，泄露个人银行帐号、密码等机密信息，造成重大经济损失。

- 带宽占用，工作效率降低

员工访问WEB 网页时，往往会被娱乐性内容所吸引，影响工作效率。

- 法律风险

员工访问WEB 网页时，网页信息中可能带有一些与法律相抵触内容。

恶意网站

- 恶意网站产生的威胁：
  - 盗窃游戏、网银账号
  - 远程控制
  - 僵尸网络
  - 隐私泄露
  - 商业威胁



每天持续有新的恶意网站增加，高峰时>2万个/天

 Page 6



随着互联网的迅速发展，同时也使其变得异常脆弱。基于WEB的攻击已经成为攻击者的首要攻击方式，网站攻击的途径不仅仅是非法网站，任何网站都有可能遭到攻击者的威胁，从而变成攻击者危害用户的“帮凶”。攻击者通过入侵合法网站并发布恶意脚本链接或恶意软件，以此攻击终端用户的计算机。

所谓恶意网页，是指网页的内容中被嵌入恶意代码，当用户访问恶意网页时，恶意代码被植入用户的计算机，可能会导致用户计算机上的隐私信息泄露，计算机成为僵尸网络等严重问题。

- WEB攻击

基于WEB的攻击已经成为攻击者的首要攻击方式，攻击者通过入侵合法网站并发布恶意脚本链接或恶意软件，以此攻击终端用户的计算机。

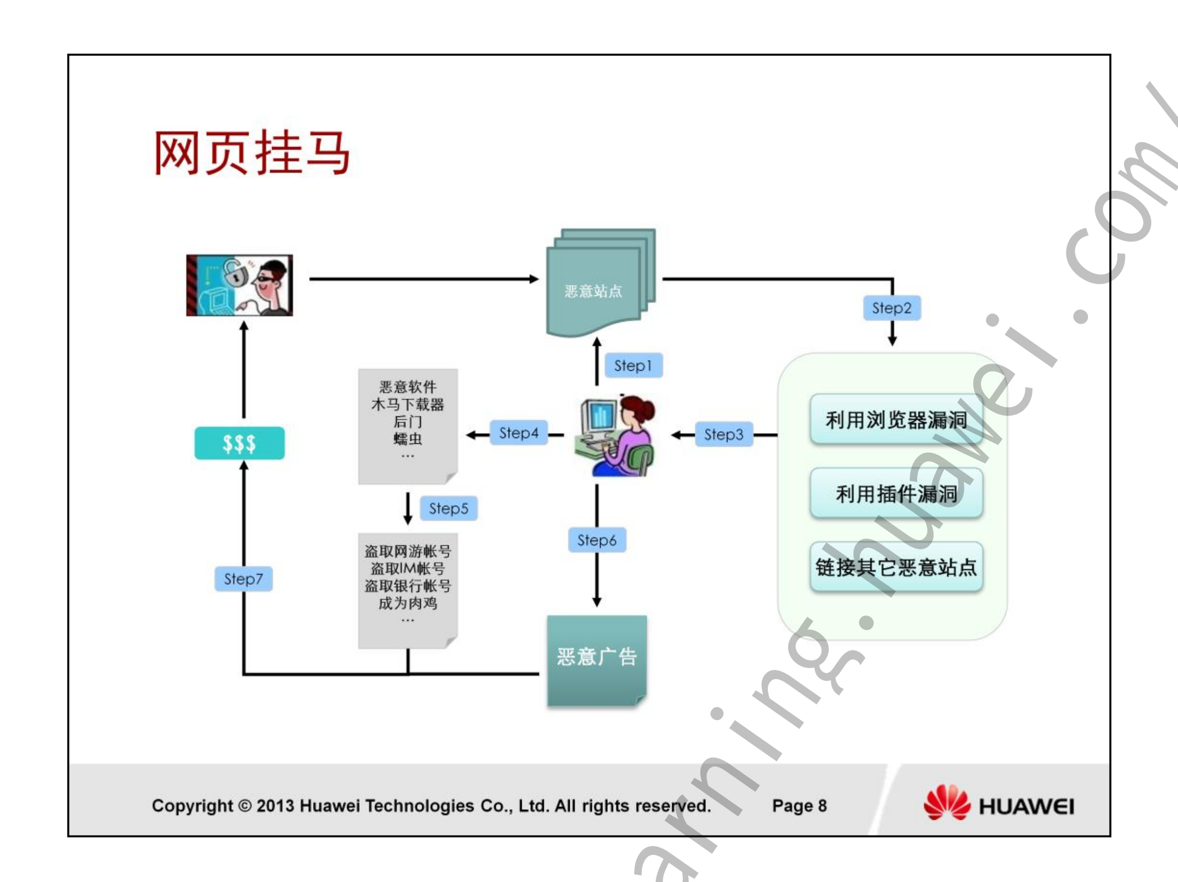
- 恶意网页

网页的内容中被嵌入恶意代码，当用户访问恶意网页时，恶意代码被植入用户的计算机，可能会导致用户计算机上的隐私信息泄露，计算机成为僵尸网络等严重问题。

漏洞



- WEB相关威胁和问题—热点漏洞举例：
  - Microsoft DirectShow 组件栈溢出漏洞；
  - MICROSOFT OFFICE WEB 组件内存破坏漏洞；
  - RealPlayer rmoc3260.dll ActiveX控件内存破坏漏洞；
  - Firefox 3.5 Tracemonkey组件远程代码执行漏洞；
  - Adobe Flash Player畸形SWF文件解析远程代码执行漏洞；
  - Adobe Reader AcroRd32.dll模块漏洞。



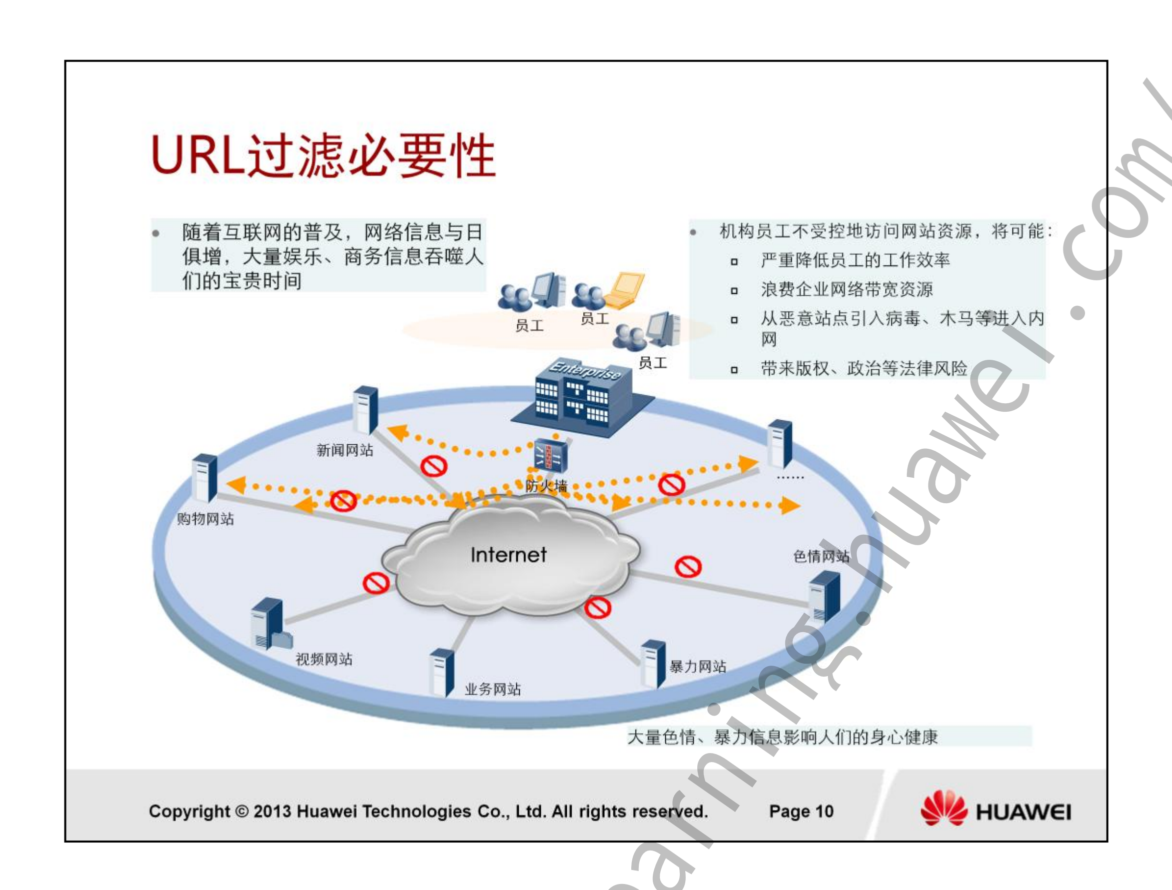
- 网页挂马流程:
  - 客户端PC上网浏览到一些恶意站点，触发了该恶意网页的运行;
  - 这个网页木马被执行后，就会利用浏览器漏洞、插件漏洞进行破坏行动，或者链接其它恶意站点;
  - 下载在恶意攻击行为者事先准备的木马软件;
  - 通过利用浏览器等漏洞，在后台自动下载指定位置的木马并安装或直接运行。这些过程都在后台运行,用户很难察觉的到。实际上虽然考虑到安全问题,浏览器是禁止自动下载程序的,但是浏览器总是存在一些已知或未知的漏洞,网页木马就是利用这些漏洞来获得下载程序或运行程序的权限的;
  - 木马运行后在客户端PC上秘密运行收集客户端PC的重要隐秘信息，比如网游、IM、银行等帐号;
  - 同时或通过恶意网站链接恶意广告;
  - 最终成为恶意行为制造者经济利益收获的使用工具。
- 简单来说，网站挂马一般可以简化为以下三个流程:
  - 制作黑页：针对客户端软件存在的漏洞，黑客构建的包含恶意代码的网页;
  - 网站挂马：利用SQL注入、XSS跨站脚本等攻击入侵合法网站并嵌入可跳转到黑页的链接;
  - 下载木马：客户端访问被挂马网站，并跳转到黑页，这是由于客户端软件存在漏洞会执行恶意代码自动下载木马软件。

上述流程涉及了三个主体：被挂马网站、黑页（也叫做挂马源）、有漏洞的客户端软件，要解决网站挂马问题，就要从这三方面入手。

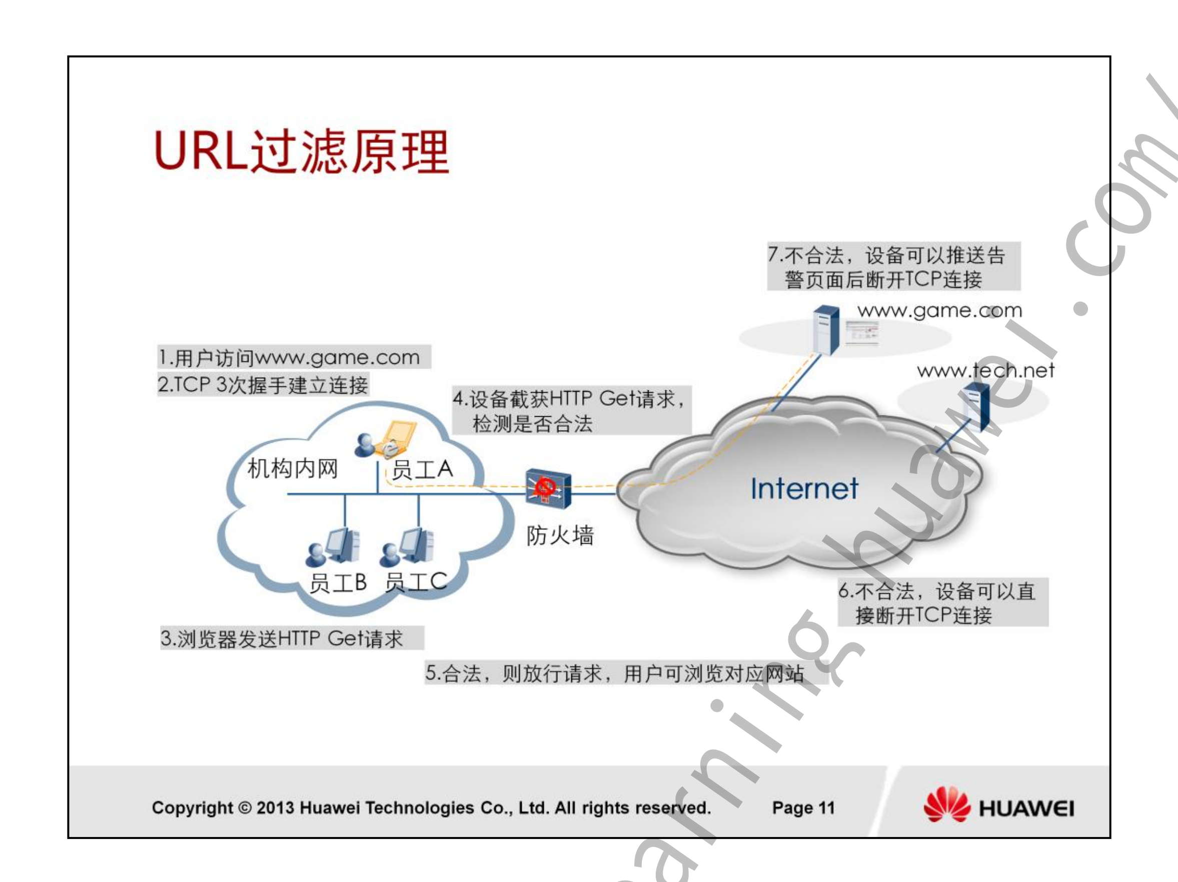


目录





URL过滤技术对用户的HTTP请求进行访问控制，允许或禁止用户访问某些网络资源，可以达到规范上网行为的目的。



- 网关设备URL过滤的原理：
  - 截取用户HTTP连接Get或POST请求，根据用户配置策略判断其合法性；
  - 如果URL合法，则该HTTP请求被放行，用户可以浏览网站；
  - 如果URL不合法，则对该HTTP连接进行告警页面推送并且阻断。



Internet上的每一个网页都具有一个唯一的标识，称为URL（Uniform Resource Locator）地址。

URL地址用来完整地描述Internet上网页和其他资源地址。简单地说，URL就是WEB地址。

- URL格式：protocol://hostname[:port]/path[? query]
  - protocol：最常使用的是HTTP协议。对于HTTP协议，一般可不输入；
  - hostname：WEB服务器的DNS主机名或IP地址；
  - port：可选，通信端口。各种传输协议都有默认的端口号；
  - ? query：可选，用于给动态网页传递参数。

URL匹配方式

匹配方式	条目	匹配结果
前缀匹配	www.huawei.com	匹配所有以www.huawei.com开头的URL，如：www.huawei.com、www.huawei.com/solutions.do
后缀匹配	aspx	匹配所有以aspx结尾的URL，如：www.huawei.com/news/solutions.aspx、www.huawei.com/it/price.aspx
关键字匹配	huawei.com	匹配所有包含huawei.com的URL，如：www.huawei.com/news/solutions.aspx、www.huawei.com/it/
精确匹配	www.huawei.com/news	只匹配www.huawei.com/news。www.huawei.com/news/solutions.aspx、www.huawei.com/news/en/等不会匹配该条目
参数匹配	a-param	匹配所有参数中包含a-param的URL，如：www.huawei.com/education.aspx?#$%a-param^&、www.huawei.com/news/en/political?a-parameter，但是不会匹配www.a-param.com、www.huawei.com/a-param



前4种匹配针对于hostname/path部分，参数匹配针对于query部分，可用于匹配搜索引擎搜索关键字,注意URL只对HTTP协议数据进行过滤。

黑白名单过滤

匹配方式	白名单	黑名单
前缀匹配	支持	支持
后缀匹配	支持	支持
关键字匹配	支持	支持
精确匹配	支持	支持
参数匹配	不支持	支持



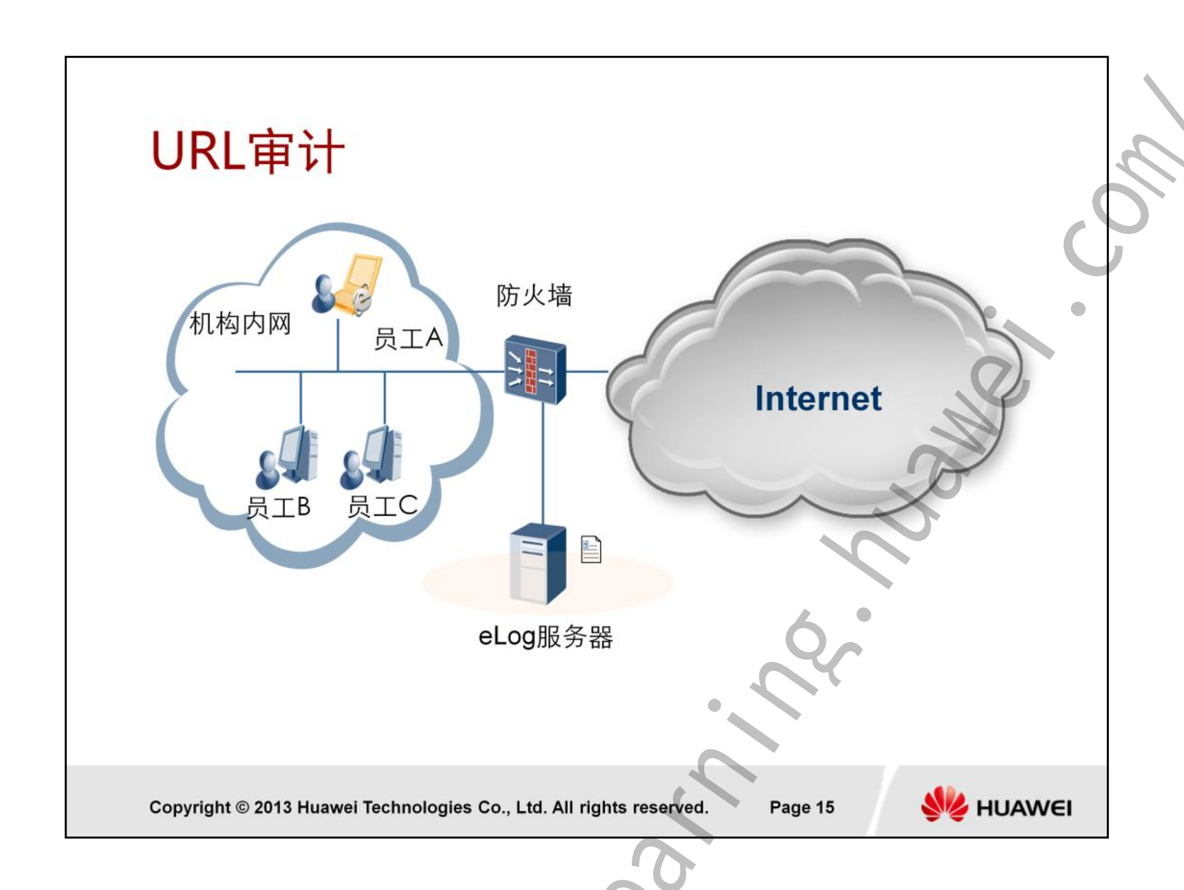
设备将HTTP上网请求的URL与黑白名单进行匹配，如果匹配白名单则允许该HTTP请求，如果匹配黑名单则阻止该HTTP请求。

当上网请求的URL与白名单匹配时，不会再进行后续的处理（包括AV、IPS等）。设置白名单有利于提高匹配效率。

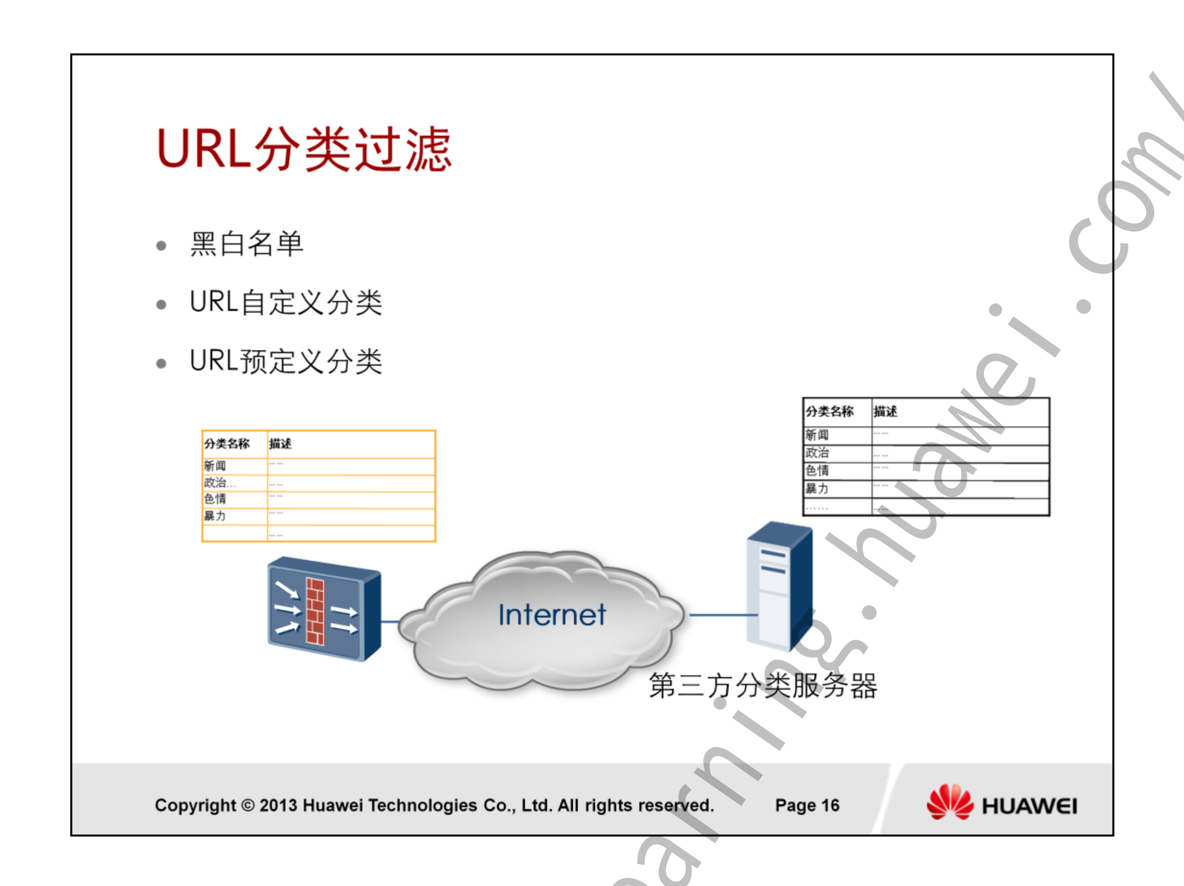
- 设备将HTTP上网请求的URL与黑白名单进行匹配
    - 如果匹配白名单则放行该HTTP请求；
    - 如果匹配黑名单则阻断该HTTP请求，同时显示阻断页面通告。
- 使用多种匹配方式，可灵活地允许或者禁止对URL访问

注：为了禁止使用搜索引擎搜索某些关键字，黑名单支持参数匹配方式

通过豁免IP功能可以使特定的IP地址集不进行黑白名单过滤、自定义分类过滤、预置分类过滤，直接放行，针对特殊用户使用。



- URL审计功能用来记录用户的HTTP上网行为，并作为审计依据
- 用户可配置需要审计的WEB资源类型，WEB资源类型以文件扩 展名来区分，包括html 、jsp、aspx等
- 内部用户访问指定类型的WEB资源，防火墙将记录日志并发送给日志服务器



- 黑白名单

设备将HTTP上网请求的URL与黑白名单进行匹配，如果匹配白名单则允许该HTTP请求，如果匹配黑名单则阻止该HTTP请求。

当上网请求的URL与白名单匹配时，不会再进行后续的处理（包括AV、IPS等）。设置白名单有利于提高匹配效率。

- URL自定义分类，即本地URL过滤

URL自定义分类由用户自行配置和维护。URL自定义分类将具有相同特征的URL进行分类，用户可以根据业务配置策略，允许或拒绝各个分类URL的访问。相对于预定义URL分类，用户可以使用自定义分类对URL进行更为精细化的控制。

- URL预定义分类，即远程URL过滤

URL预定义分类由安全服务中心提供并维护。URL预定义分类中定义了各种URL的分类，例如教育类URL、新闻类URL，用户可以根据业务使用策略，允许或拒绝各个分类网站的访问。使用URL预定义分类的情况下，需要建立到安全服务中心的连接。相对于需要用户自行配置的自定义分类，预定义分类已经预先对大量常见的URL进行了分类，用户可以根据这些分类轻松地控制内网用户禁止访问哪些类别的URL、允许访问哪些类别的URL。

URL分类过滤技术

- 根据自定义分类或者预定义分类，用户可以创建多个URL策略

URL策略	描述
销售部URL控制	……
研发部URL控制	……
总工办URL控制	……
研究部URL控制	……
……	……

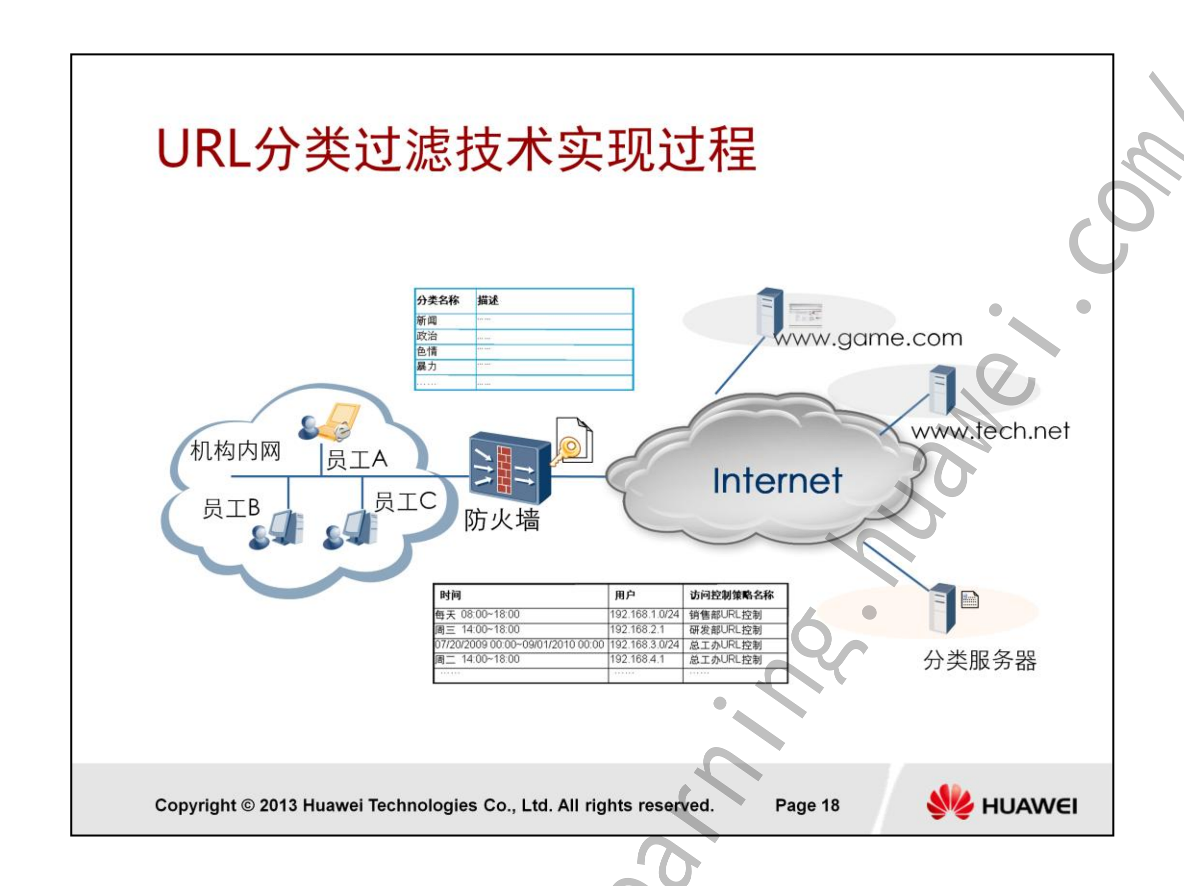
每条URL策略定义了分类的处理动作

分类名称	动作
体育	阻断
友商	允许
搜索	允许
游戏	阻断
……	……

分类名称	动作
新闻	阻断
政治	允许
色情	阻断
暴力	阻断
……	……



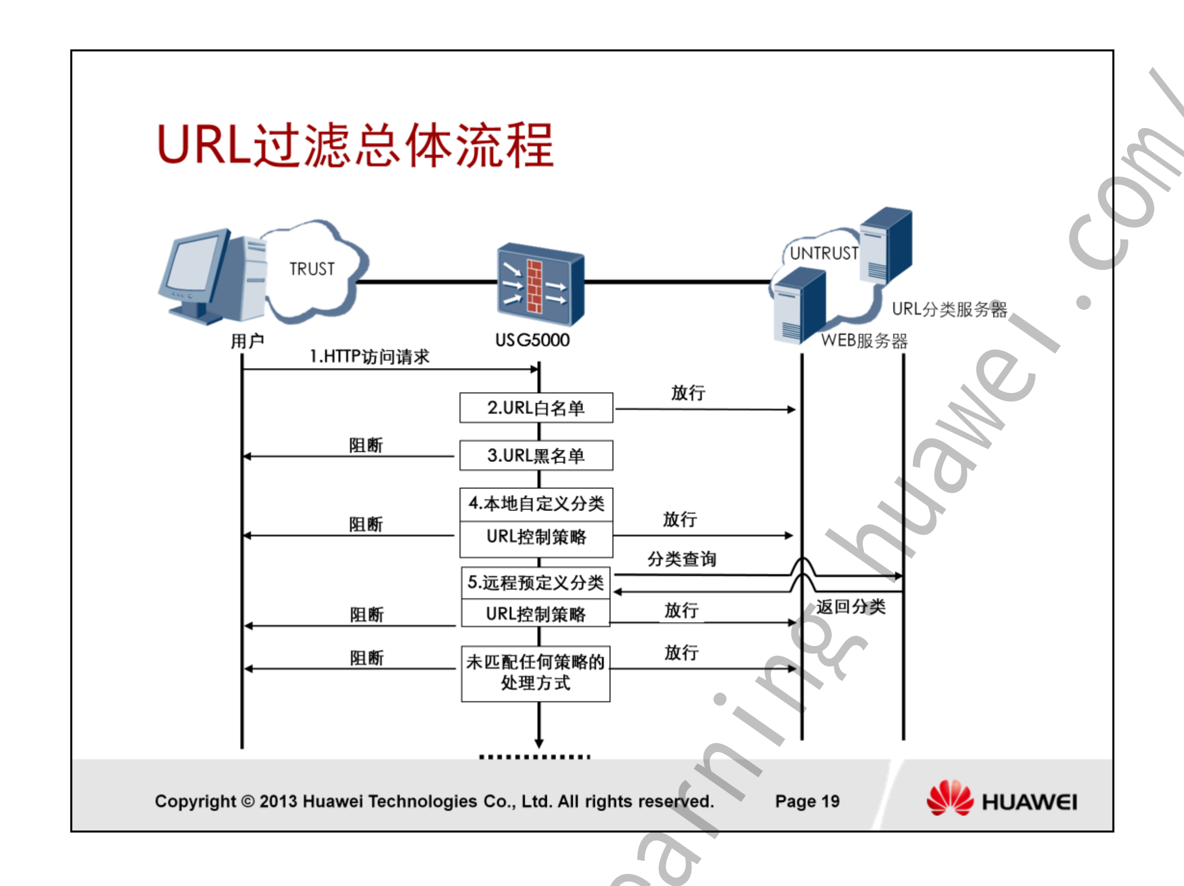
通过将URL策略引用到域间，与域间策略配合使用，实现基于时间和地址集等的URL过滤。



分类名称	描述
新闻	……
政治	……
色情	……
暴力	……
……	……

时间	用户	访问控制策略名称
每天 08:00~18:00	192.168.1.0/24	销售部URL控制
周三 14:00~18:00	192.168.2.1	研发部URL控制
07/20/2009 00:00~09/01/2010 00:00	192.168.3.0/24	总工办URL控制
周二 14:00~18:00	192.168.4.1	总工办URL控制
……	……	……

- URL分类过滤技术的实现过程:
  - 当用户通过防火墙访问外网时，防火墙首先进行本地自定义分类过滤；
  - 设备根据用户的URL从本地类别列表中得到对应的分类；
  - 找到分类后，设备根据访问控制策略中对应分类的动作，阻断或者放行URL请求；
  - 如果没有命中本地自定义分类过滤，紧接着进行远程预定义分类过滤；
  - 设备将用户URL发给分类服务器获取对应的分类；
  - 找到分类后，设备根据访问控制策略中对应分类的动作，阻断或者放行URL请求。



- 用户发起HTTP请求；
- USG5000将HTTP请求的URL与白名单中的记录进行匹配。如果匹配白名单，则放行此URL，如果未匹配白名单，则进行下一步检测；
- USG5000将HTTP请求的URL与黑名单中的记录进行匹配。如果匹配黑名单，则阻断此URL，如果未匹配黑名单，则进行下一步检测；
- USG5000将HTTP请求的URL与本地自定义分类列表中的记录进行匹配。如果匹配本地自定义分类，则根据分类过滤策略放行或阻断此URL。如果未匹配本地自定义分类，则进行下一步检测；
- USG5000将HTTP请求的URL向URL分类服务器发起远程预定义分类查询。如果匹配远程预定义分类，则根据分类过滤策略放行或阻断此URL。如果未匹配远程预定义分类，则根据未匹配任何过滤策略的处理方式放行或阻断此URL。如果服务器连接失败或者查询超时，则根据服务器查询失败处理方式放行或阻断此URL；
- 如果启用了URL审计功能，USG5000对URL中的资源类型进行审计。如果URL中的资源属于用户配置的审计资源类型，则USG5000将此URL信息发送到审计服务器。



目录





- 搜索关键字过滤技术是指对指定搜索关键字进行过滤，控制内网用户的搜索内容，防止用户获得敏感信息。





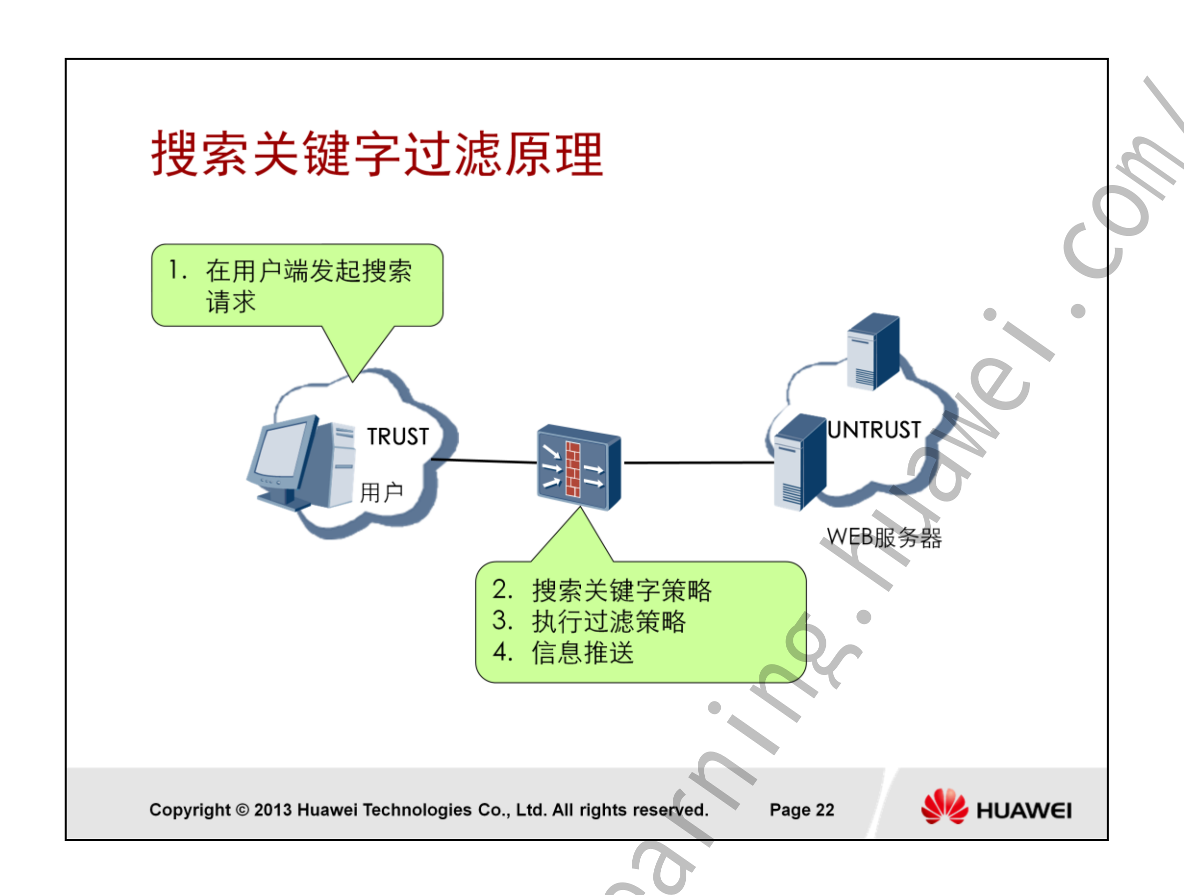






据调查显示，搜索引擎是网民访问量最大的网站类型之一，用户大多数的web站点访问行为都是从搜索引擎开始的，目前支持的搜索引擎有Google、Yahoo、Bing、百度。

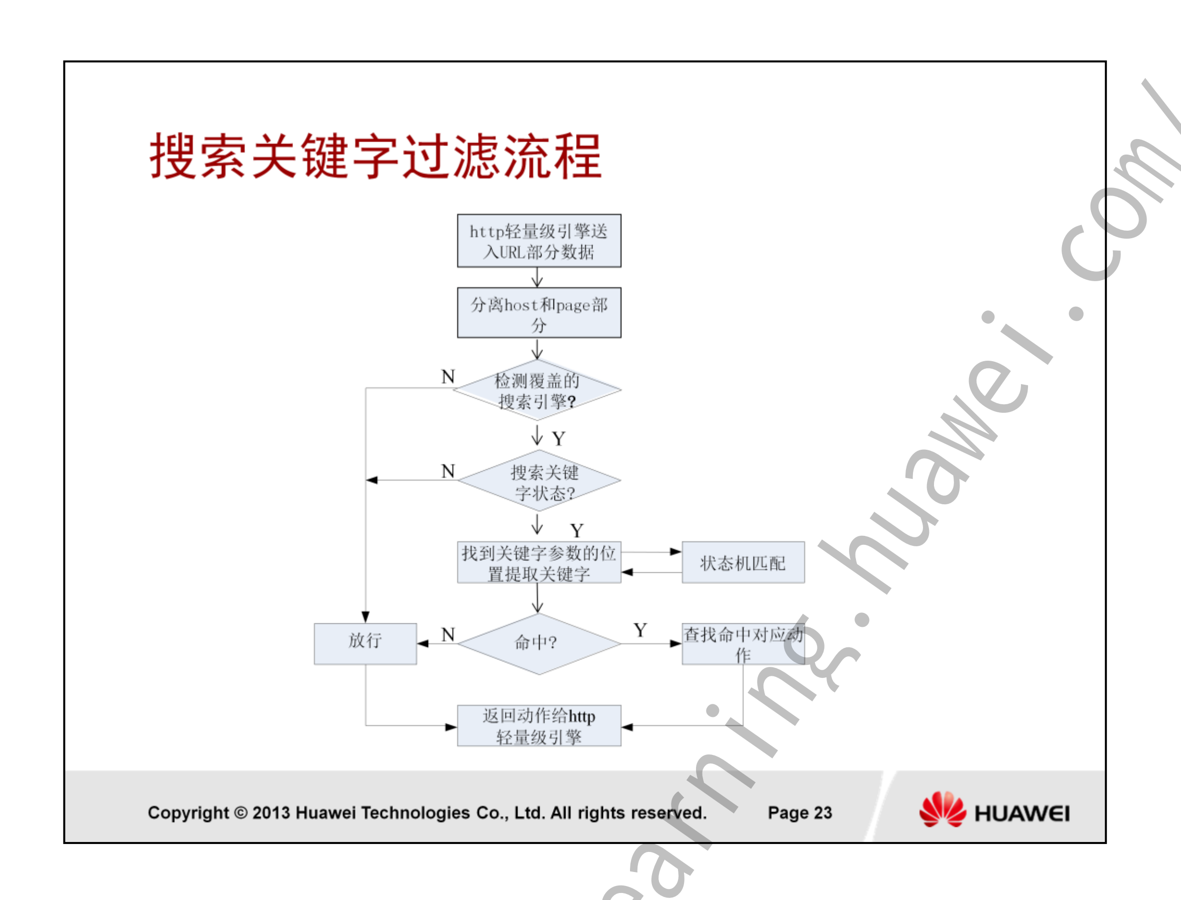
对于企业来说，员工日常进行的检索活动能够反映其近期的生活情况和情绪状态，如果企业员工在上班时间不受限制的访问网络，不但会占用上班时间，影响工作效率，还有产生信息安全问题，乃至影响组织信誉和法律问题。 “搜索引擎关键字过滤技术”功能恰好可以帮助企业用户解决这一难题。通过设置针对性策略，企业用户可以对搜索引擎关键字检索行为进行封堵，能够从源头上减少用户访问不良网站、获取不良信息。从而互联网资源的极大丰富，方便了资源的共享，提高了工作效率。



搜索关键字过滤是指对指定搜索关键字进行过滤，控制内网用户的搜索内容，防止用户获得敏感信息。防火墙上开启搜索关键字过滤功能后，当用户在搜索引擎上搜索内容时，防火墙会对该HTTP报文进行解析：

- 如果匹配搜索关键字策略，执行过滤策略（阻断或告警）；同时可以选择向用户推送Web页面，提醒用户访问受限。
- 如果没有匹配搜索关键字策略，则允许该HTTP报文通过。用户可以正常进行搜索。

当搜索的关键字中出现“&”和“=”字符时，可能会躲避过检测。



搜索关键字过滤技术是对指定搜索引擎中的关键字进行过滤，控制内网用户的搜索内容，搜索关键字过滤技术执行WEB过滤使用以下方法：

- 当HTTP轻量级流量送入url部份数据，首先要分离HOST和page部份；
- 检测覆盖的搜索引擎，如果不检测覆盖的搜索引擎将对HTTP流量放行，反之，将搜索关键字状态进行检测；
- 如果不检查搜索关键字状态将对HTTP流量放行，反之，找到关键字参数的位置提取关键字与状态机进行匹配；
- 如果提取的关键字没命中状态机将对HTTP流量放行，相反将查找命中对应动作，返回动作（阻断、告警、不处理）给HTTP轻量级引擎。



目录



WEB内容过滤技术介绍

- Web内容过滤对用户访问Web页面的内容进行控制。
  - 网页浏览关键字
  - HTTP POST过滤
  - HTTP POST文件过滤
  - 上传/下载文件名关键字
  - 上传/下载文件类型关键字
  - 文件大小过滤



Web内容过滤对用户访问Web页面的内容进行控制。

- 网页浏览关键字：过滤网页上的内容。
- HTTP POST关键字：过滤HTTP POST操作。
- 上传/下载文件名关键字：根据上传或下载的文件名进行过滤。
- 上传/下载文件类型关键字：根据上传或下载的文件类型进行过滤。
- 文件大小过滤：根据上传或下载的文件大小进行过滤。

网页浏览关键字、文件名支持关键字对象组匹配（任意匹配）。例如，假设管理员在设备上配置了禁止浏览关键字“暴力”的网页，那么用户将不能访问包含“暴力”的网页

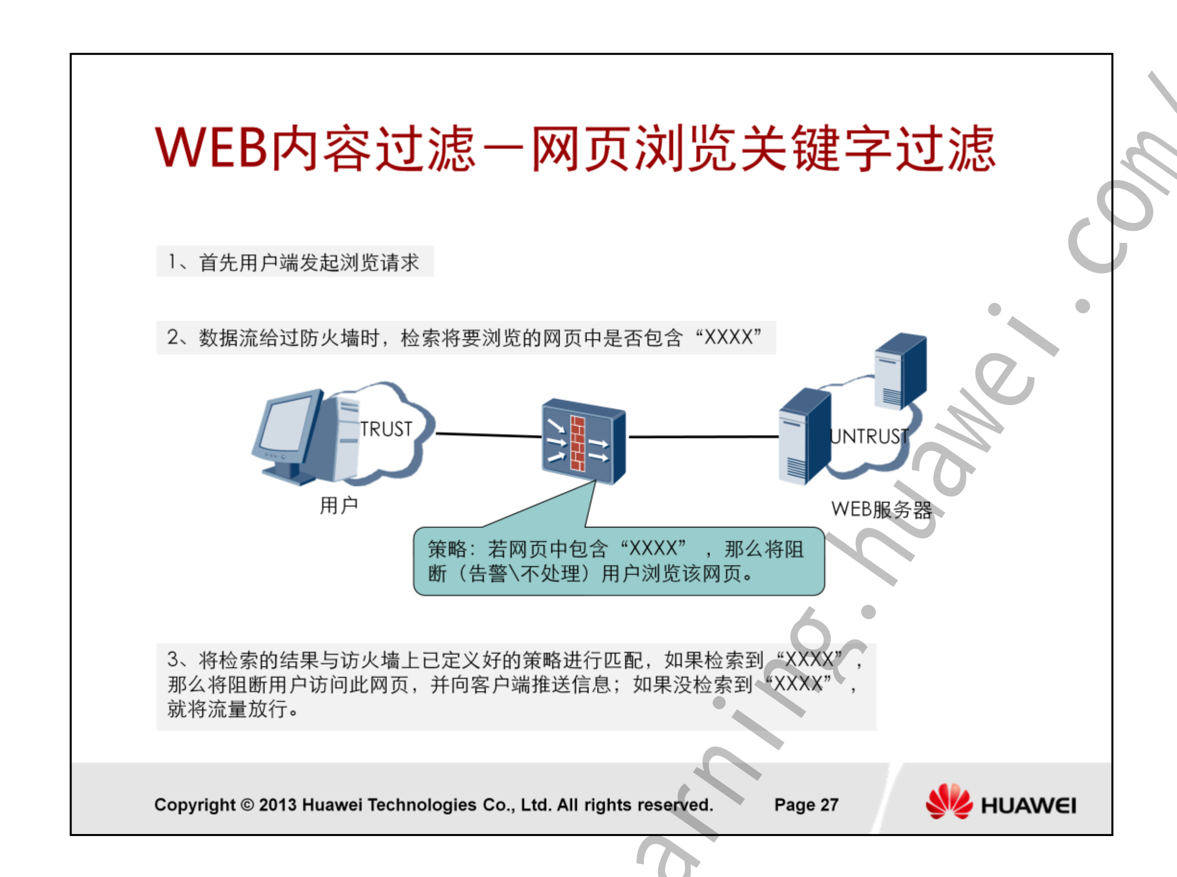
文件类型支持文件类型对象组匹配（精确匹配）。例如，假设管理员在设备上配置了禁止下载文件类型为mp3的文件，那么用户将不能下载文件类型为mp3的文件，但能下载文件类型为mp的文件。

注：文件大小不匹配公共对象组。

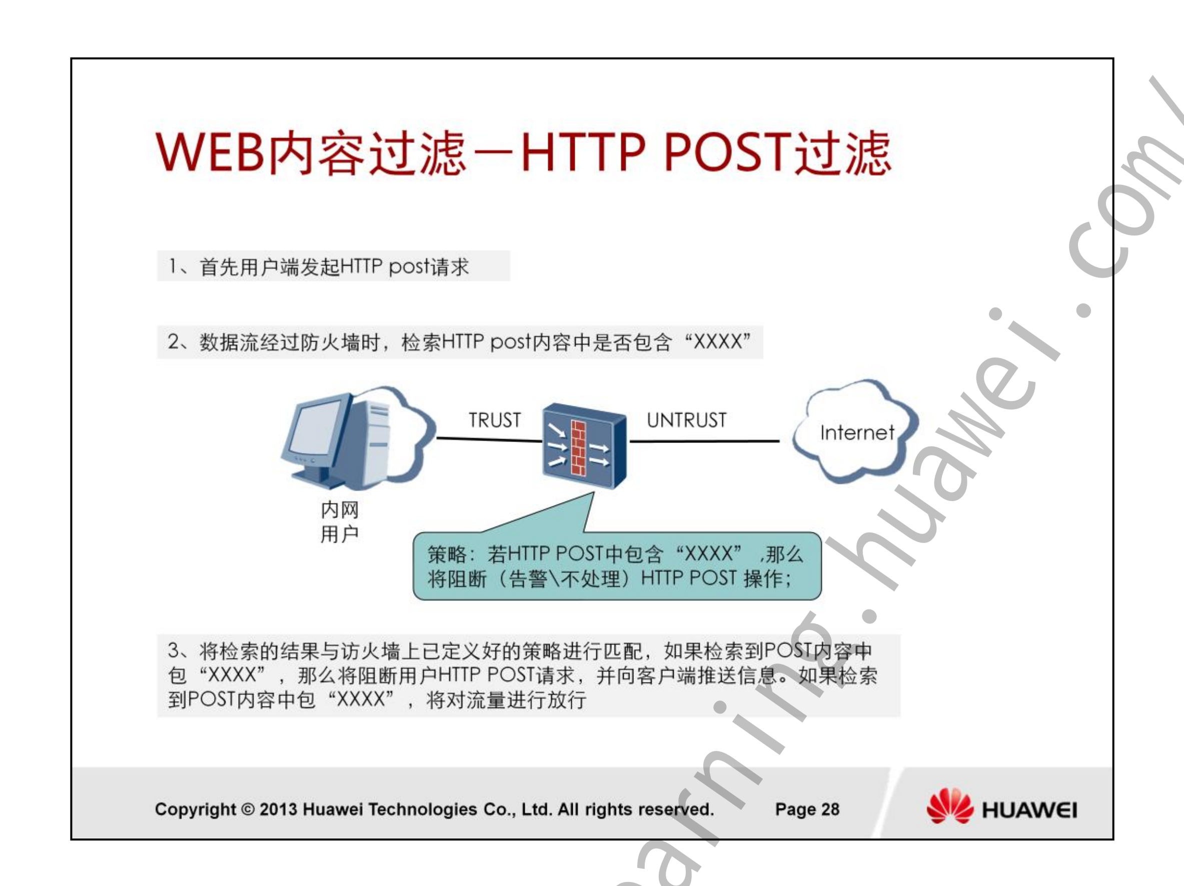
WEB内容过滤原理

- 用户发起上传附件的操作，触发发送HTTP报文。
- HTTP报文经过防火墙时，防火墙会对其进行过滤：
  - 如果匹配上传文件名关键字策略，执行过滤策略（阻断或告警）；同时可以选择向用户推送Web页面，提醒用户访问受限。
  - 如果没有匹配上传文件名关键字策略，则允许该HTTP报文通过。用户可以正常上传该文件。





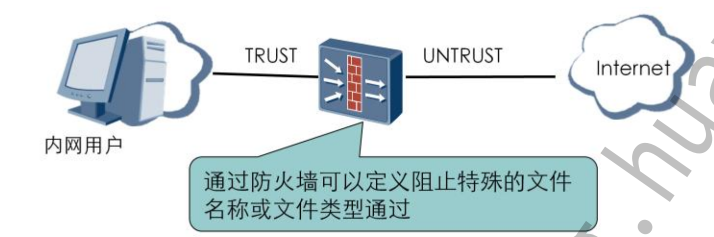
网页浏览关键字过滤是WEB内容过滤技术之一，主要是针对用户所浏览的网页中是否包含违规或不健康信息，当用户访问到这一类信息，防火墙将会对此做出相应的应对措施



HTTP POST（文件）过滤技术是WEB内容过滤技术这一，我们在访问网页时会涉及到GET和POST两个方向的请求，在这里将介绍对POST业务方面进行过滤，涉及POST操作有论坛、EMAIL等；对于一个企业来说，为了保信息信息安全，防止内网用户向外部用户发送公司的机密信息，那么就通过对POST的关键字和附件进行过滤，从而降低信息安全隐患

WEB内容过滤－上传/下载关键字过滤

- 上传/下载关键字包括：
  - 文件名，可以是任何文件名称；
  - 文件类类型，如：doc 、mp3等；

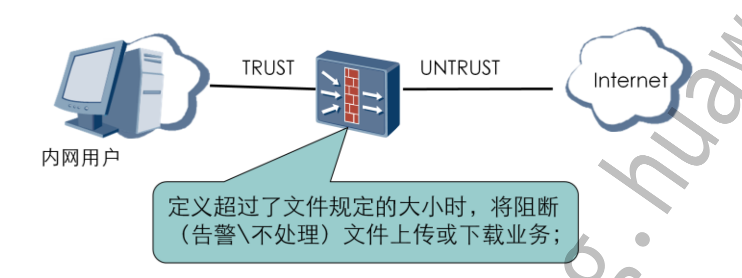




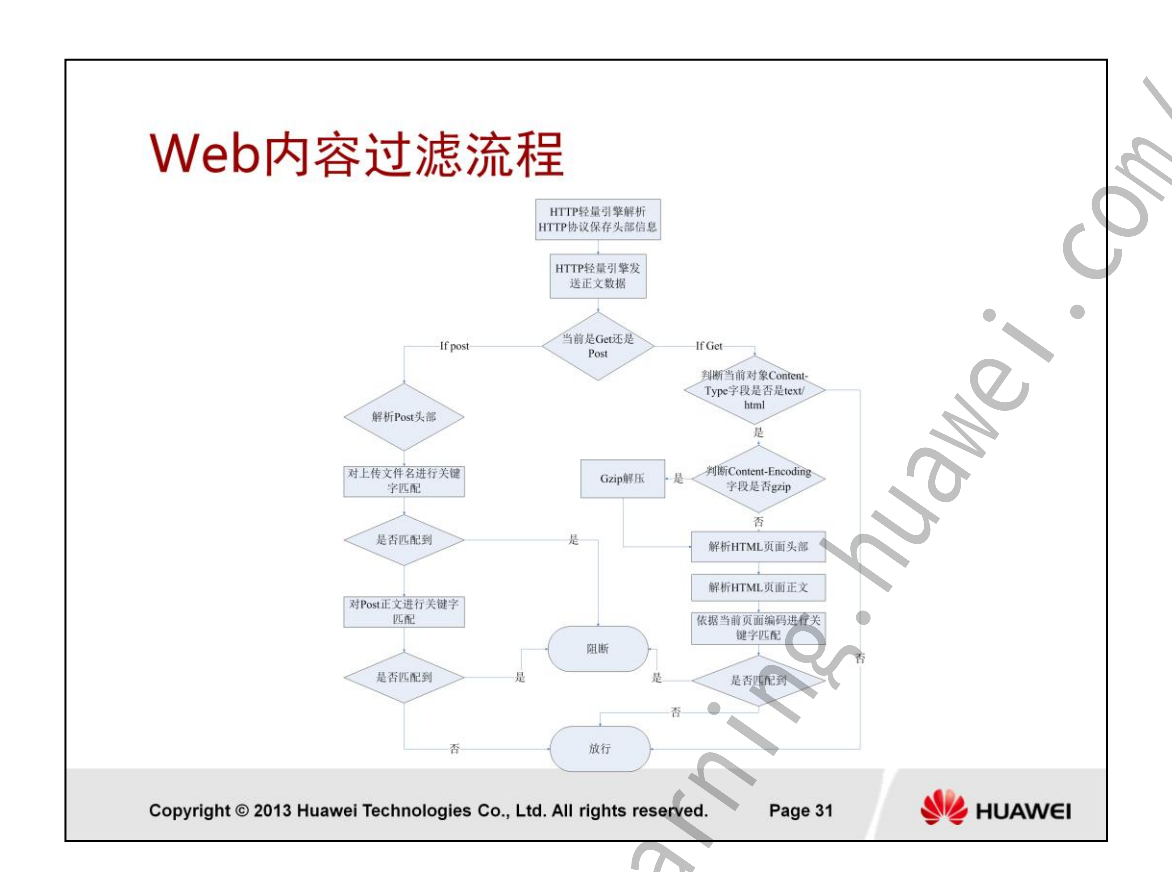
通过防火墙可以定义阻止特殊的文件名称或文件类型通过

WEB内容过滤－文件大小过滤

- 文件大小过滤技术主要是针对文件的大小进行WEB内容过滤，当文件超过规定的大小时，将阻断（告警\不处理）文件上传或下载业务，如果小于或等于该文件大小时，将放行文件。



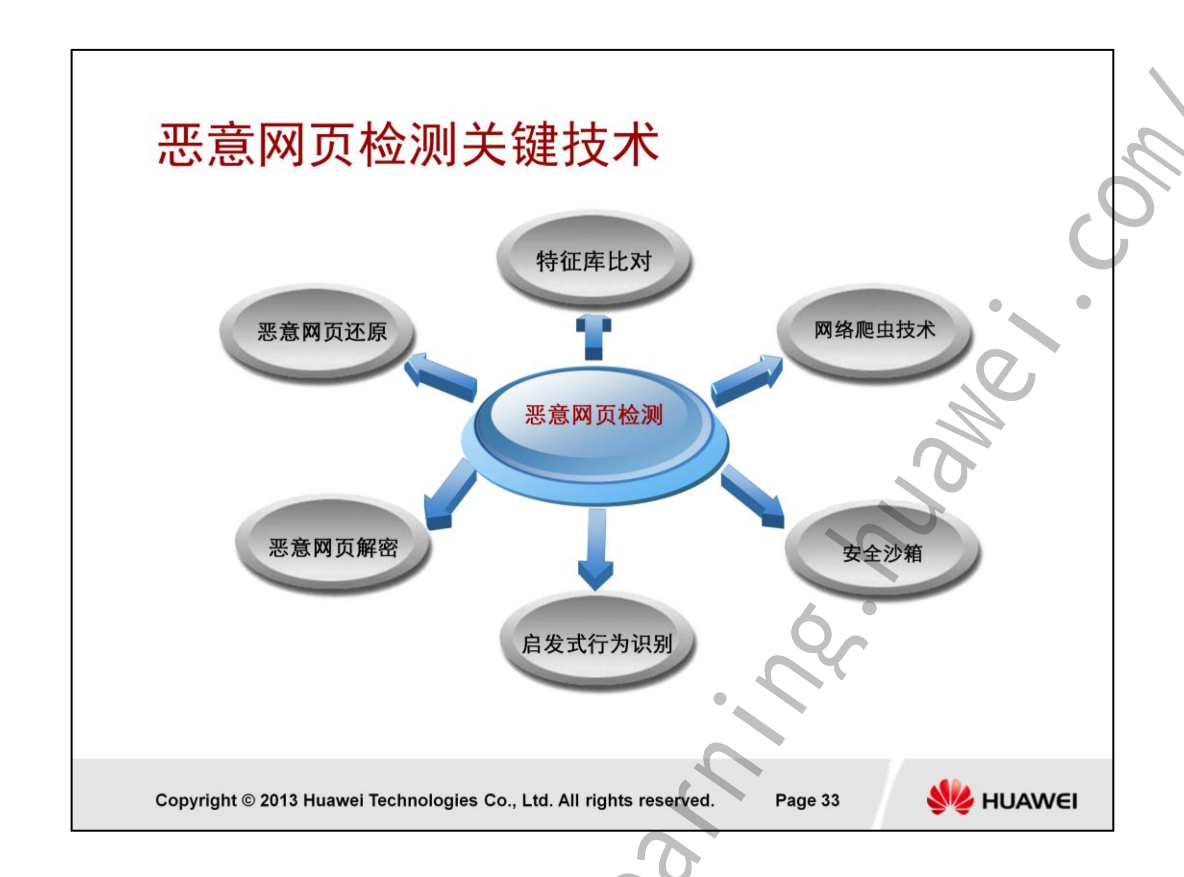



Web内容过滤流程
HTTP轻量引擎解析HTTP协议保存头部信息
HTTP轻量引擎发送正文数据
当前是Get还是Post
If post
If Get
判断当前对象Content-Type字段是否是text/html
是
解析Post头部
对上传文件名进行关键字匹配
Gzip解压
是
判断Content-Encoding字段是否gzip
否
是否匹配到
是
解析HTML页面头部
解析HTML页面正文
对Post正文进行关键字匹配
依据当前页面编码进行关键字匹配
阻断
否
是否匹配到
是
是
是否匹配到
否
否
放行
Page 31
HUAWEI



目录





- 恶意网页还原

　　针对恶意网页采用的页面拆分、函数变换、代码变形等技术，在对页面进行分析时对变形的代码进行还原。

- 特征库比对

　　生成包括上下文关系及多个特征串关联的特征匹配库 ，通过对页面的特征进行比对，识别恶意URL。

- 网络爬虫技术

　　高效爬取网页，获得网页的原始代码及相关链接，为后继的恶意网页代码分析打下基础。

- 安全沙箱

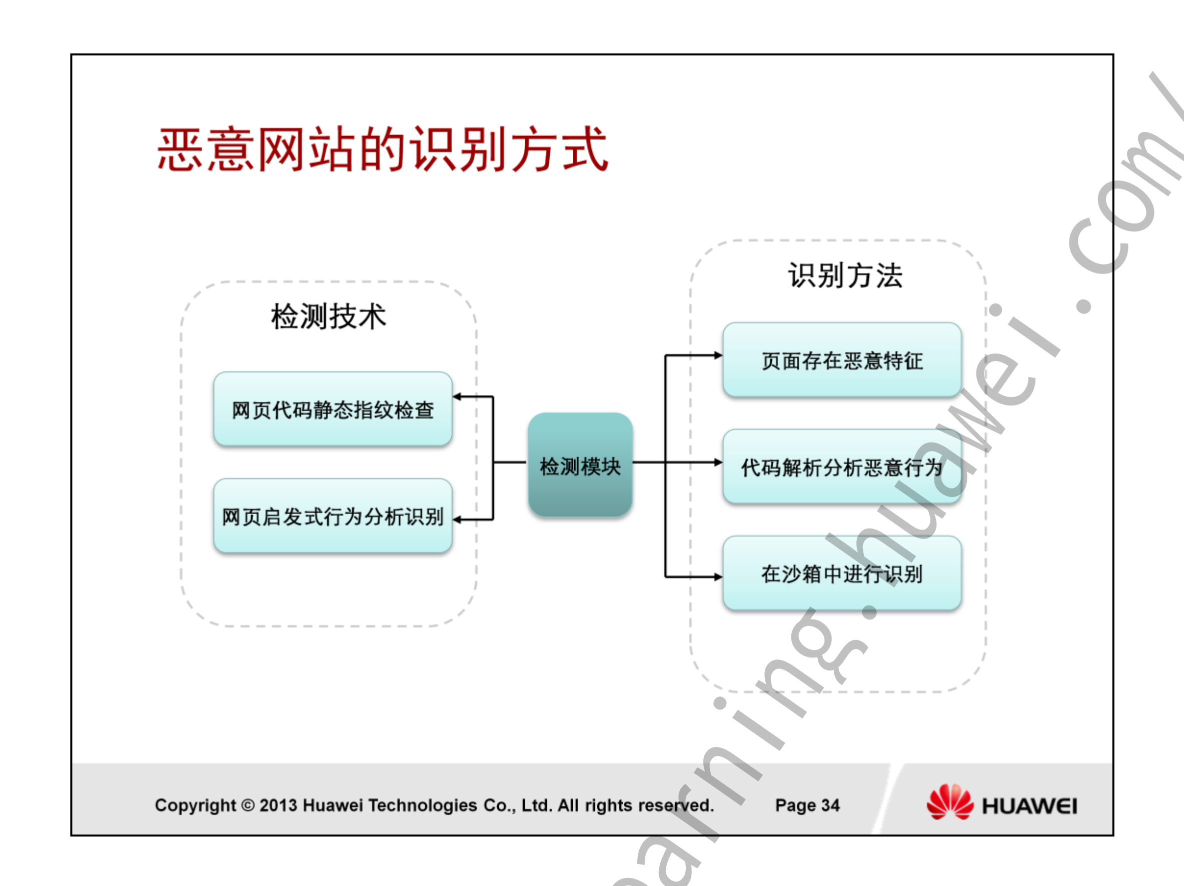
　　安全沙箱技术对疑似恶意页面进行隔离分析，能对未识别的网页提取新的挂马技术特征。

- 启发式行为识别

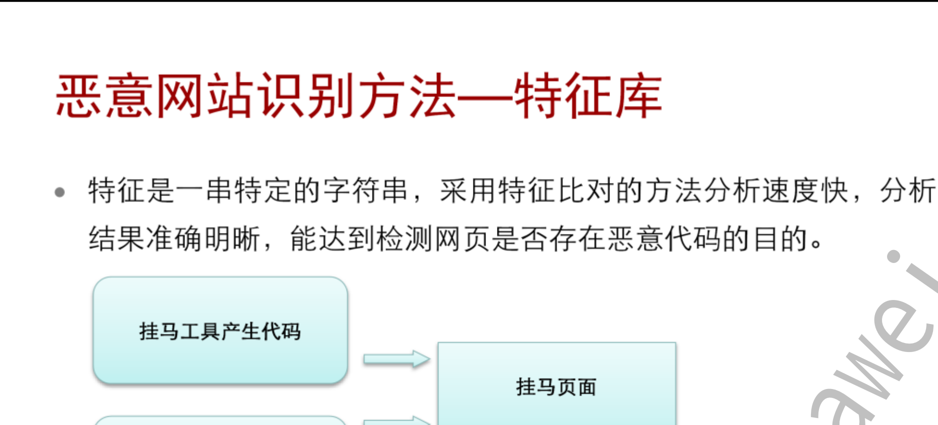
　　针对恶意网页挂马的一些典型技术，使用启发式的方法进行判断，并对最终网页木马来源进行跟踪，达到识别的目的。

- 恶意网页解密

　　针对恶意网页代码的脚本加密、工具加密、自定义加密函数等加密技术，使用脚本解密技术对恶意网页代码解密。



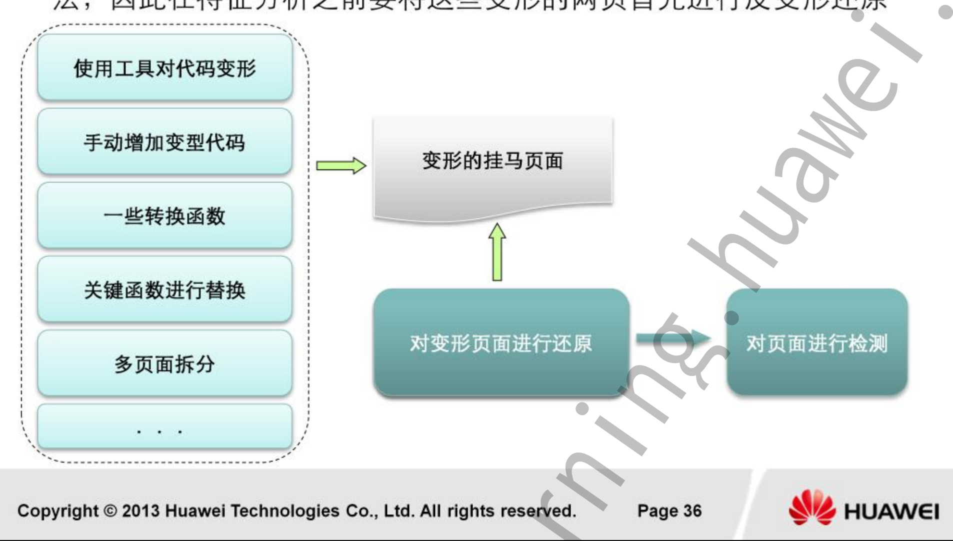
- 华为安全能力中心的自动检测模块使用了启发式分析和行为分析两种方式。
    - 特征分析是指对恶意样本进行代码静态指纹比对，而行为分析则是将恶意代码放入沙箱（Sandbox）中运行，识别其关键恶意行为。
    - 启发式行为识别，针对恶意网页挂马的一些典型技术，使用启发式的方法进行判断，并对最终网页木马来源进行跟踪，达到识别的目的。





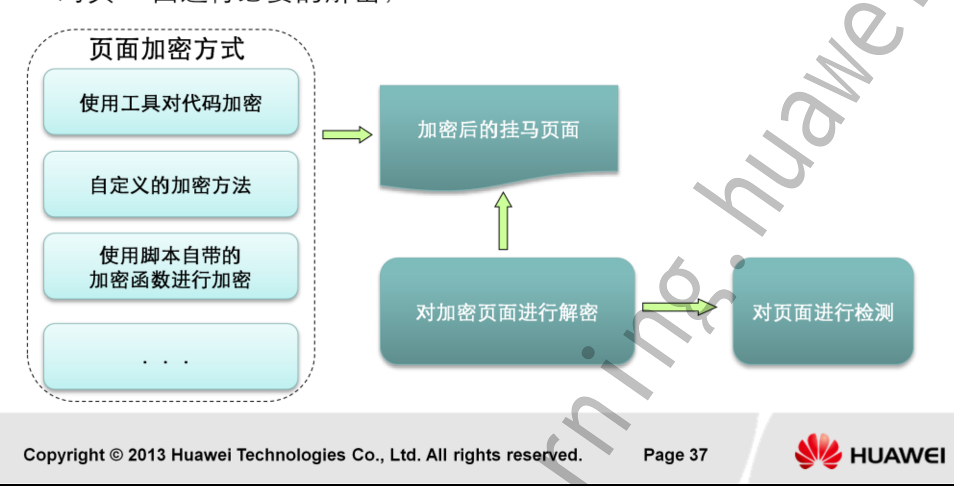
- 特征库比对

经过安全沙箱分析及人工分析的长期积累形成了恶意网页代码特征库，通过对页面的特征进行比对，识别恶意URL。恶意网页代码特征不是一个简单的字符串，而是包括了上下文关系及多个特征串关联的一种特征匹配库。



- 恶意网页代码还原技术

针对恶意网页采用的页面拆分、函数变换、代码变形等技术，在对页面进行分析时对变形的代码进行还原。

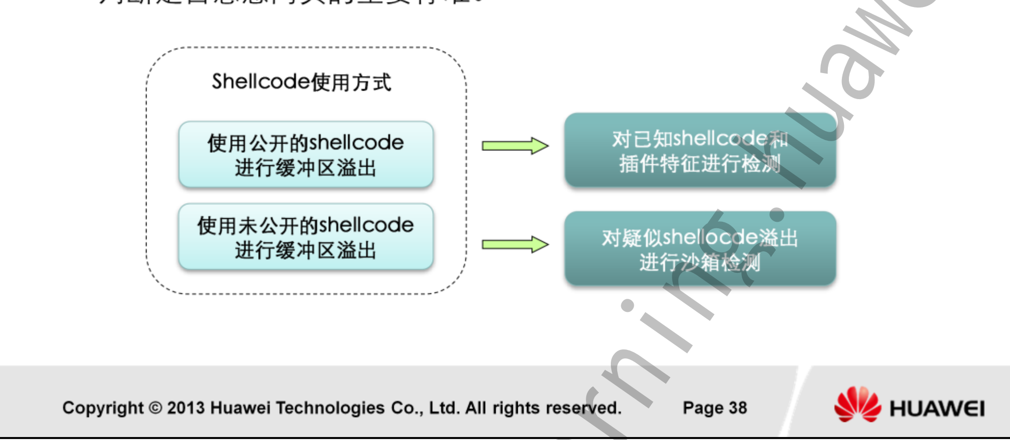


- 恶意网页代码解密技术

针对恶意网页代码的脚本加密、工具加密、自定义加密函数等加密技术，使用脚本解密技术对恶意网页代码还原，达到多层次跟踪判断的目的。

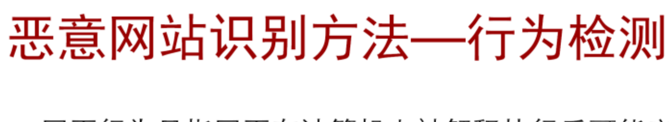
恶意网站识别方法—Shellcode

- Shellcode是一段缓冲区溢出代码，通常和ActiveX插件配合使用，用来溢出具有漏洞的计算机，达到黑客控制目的，一段Shellcode会被多个恶意网页引用，网页中是否存在shellcode是判断是否恶意网页的重要标准。



基于shellcode的防护方法是总多防护方法的一种，是从shellcode的角度出发对缓冲区溢出攻击进行检测并防御，这种方法也不可能万无一失，为保证系统安全，建议同其他措施配合使用以提高系统安全性，比如对系统进行配置，关闭不必要的服务，隐藏系统信息以降低攻击成功率，及时安装补丁程序，防止已知漏洞攻击，安装防火墙以限制远程攻击者对本地系统的连接，同时，系统使用者也要提高警惕，定期对系统进行全面的检查以确保系统安全。

检测并预防shellcode是阻止缓冲区溢出攻击成功的最后一道防线，在其他防御技术失败的情况下能够保护系统的安全，在缓冲区溢出漏洞完全消除前具有非常重要的价值，当然，这种技术还存在不足，如何能在不影响系统和程序的正常执行及性能的情况下，对shellcode作尽可能全面的监控和检查，还有待进一步完。



- 网页行为是指网页在计算机上被解释执行后可能产生的动作，比如操作文件，读写注册表等，对某些特定行为的检测可以明晰的界定一个网页是否存在恶意代码。



- 安全沙箱技术

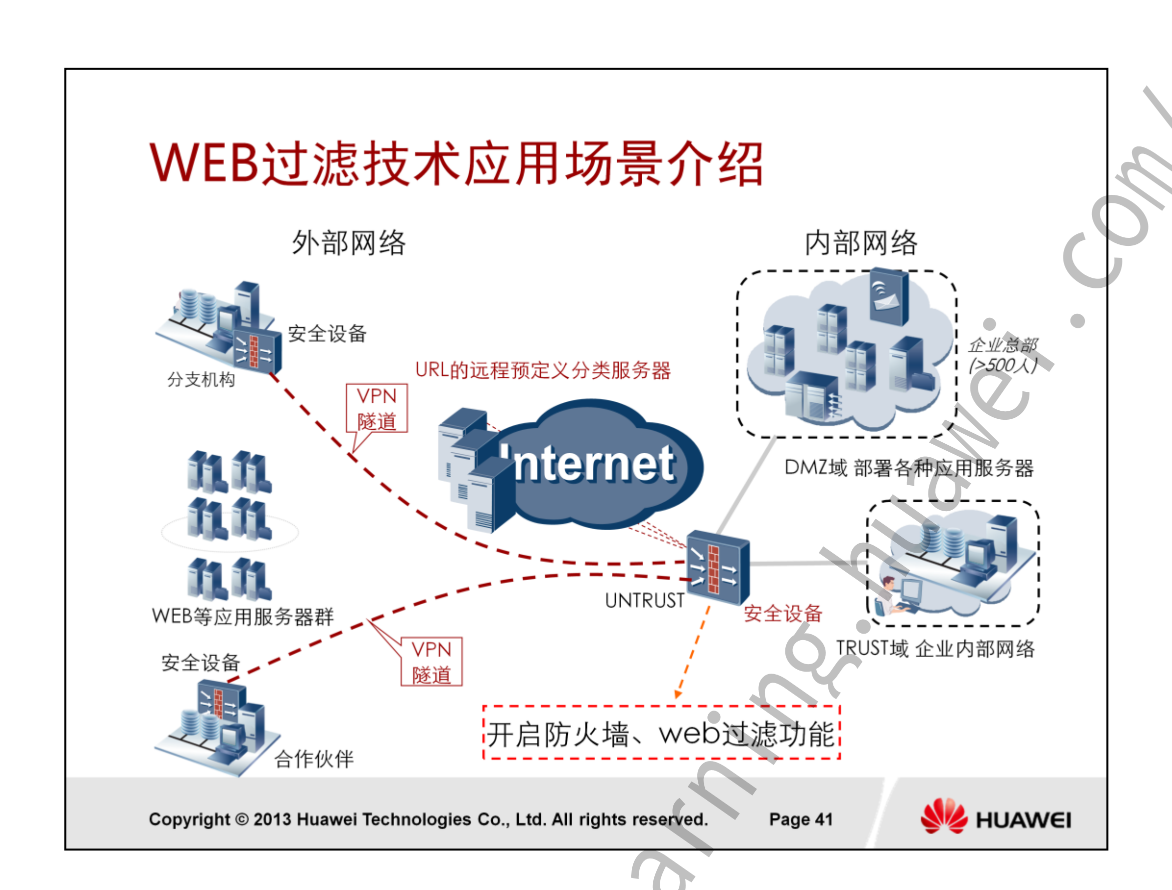
通过安全沙箱技术对疑似恶意页面进行分析，对未识别的网页提取新的挂马技术特征，形成启发式识别能力，对网页木马上下文关系和典型恶意代码特征形成特征库，达到识别新网页木马的能力。



目录



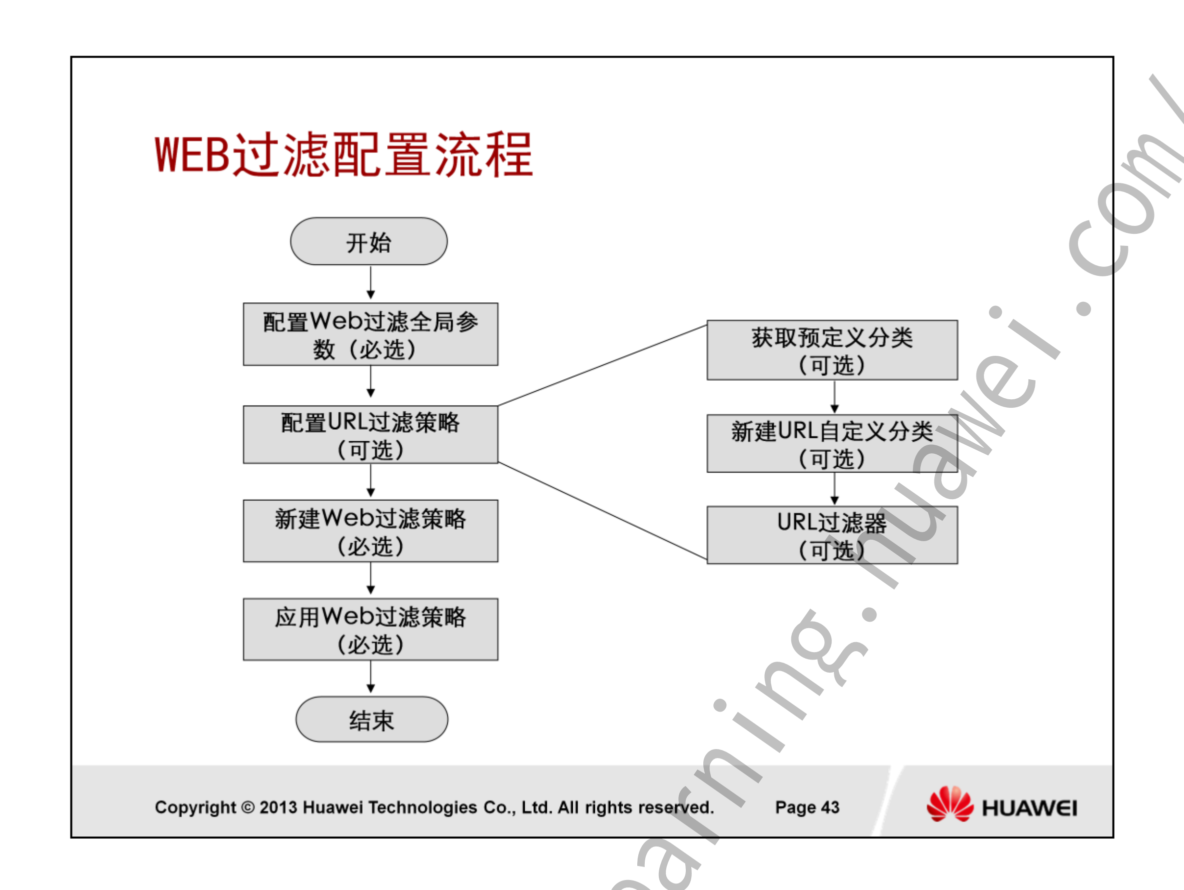



WEB过滤技术应用场景介绍
外部网络
内部网络
安全设备
分支机构
URL的远程预定义分类服务器
VPN
隧道
Internet
企业总部
(>500人)
DMZ域 部署各种应用服务器
WEB等应用服务器群
UNTRUST
安全设备
TRUST域 企业内部网络
安全设备
VPN
隧道
开启防火墙、web过滤功能
合作伙伴
Page 41
HUAWEI

WEB过滤技术应用功能列表

- 提供 WEB过滤的豁免 IP 地址集；
- 根据本地配置的黑白名单进行 WEB 过滤；
- 根据自定义分类进行 WEB过滤；
- 根据预定义分类进行 WEB 过滤；
- 支持 HTTP 访问日志记录；
- 支持功能的 license 控制。





- 配置Web过滤全局参数

Web过滤的全局参数：URL过滤、URL热点库、阻断动作、返回码、重定向URL、Web推送内容。

- 配置URL过滤策略

获取预定义分类：当需要在URL过滤中使用预定义分类，需要先获取预定义分类相关信息；

新建URL自定义分类：当需要在URL过滤中使用自定义分类时需要配置；

URL过滤器：当需要在Web过滤中使用URL过滤功能时需要配置。

- 新建Web过滤策略

可以在Web过滤中同时开启URL过滤、搜索关键字过滤和Web内容过滤。

- 配置自定义策略

在域间应用Web过滤策略后，Web过滤才真正生效。



- 选择“UTM > Web过滤 > 策略”。
- 配置全局参数。

URL过滤:只有在URL过滤功能启用的情况下，配置的URL过滤配置才生效。

URL热点库:URL热点库中保存了热点网站分类信息。通过启用URL热点库功能，可以减少远程查询分类的次数时，提升URL查询的效率

阻断动作:当用户的HTTP访问被URL过滤、搜索关键字过滤、Web内容过滤阻断时，设备采取的动作。

页面推送：将Web推送页面推送给用户。
重定向：给用户重定向到另一个URL地址。
返回码:通常情况下不需要修改。返回码的数值和含义如下:
200：请求成功
403：禁止访问
404：没有找到
406：不可接受
重定向URL：用户重定向的目的地址。例如：http://www.abcd.com:8080，只支持HTTP协议。

Web推送内容:配置Web推送的内容。

- 单击“应用”。

获取预定义分类

UTM > Web过滤 > URL分类

安全服务中心连接状态

安全服务中心连接状态: ① 未连接

URL过滤预定义分类查询服务过期时间 ② 2012/10/13 ③ 激活

URL分类列表 ④

新建 删除 刷新 | 请输入分类名称 查询

名称	描述
P2P	Web sites related to P2P
下载	Web sites related to kinds of download
人文	Web sites related to kinds of culture(arts,history,etc.)
体育/运动	Web sites related to kinds of Sports
社会焦点	Web sites related to kinds of Social Focus(social issue,ecology,human rights,etc.)
军事	Web sites related to military
社交网络	Web sites related to SNS
博彩	Web sites related to lottery
休闲	Web sites related to recreation(games,cartoon,chat,dating, etc.)
宗教	Web sites related to religion
性题材	Web sites related to sex but not porn
房产/家居	Web sites related to real estate and household

  HUAWEI

URL分类是具有相同特征的URL集合。URL分类包括两种：预定义分类和自定义分类，预定义由安全服务中心提供并维护，自定义分类由用户自行配置和维护。用户可以指定每个URL分类的控制动作，从而达到URL过滤的目的。

- 获取预定义分类

设备通过安全服务中心获取的被查询URL的预定义分类，然后根据返回的分类以及配置的分类控制动作决定是否允许该URL进行访问。缺省情况下，设备发现分类不全的情况下，才会主动向安全服务中心更新分类。

- 查看安全服务中心的连接状态。
  - 连接中：表示正在建立连接。请观察一段时间，看安全服务中心的连接状态是变成了已连接还是未连接，然后根据以下相应的状态进行处理。
  - 已连接：表示已经建立连接。系统会定时地自动从安全服务中心上获取最新的预定义分类。
  - 未连接：表示没有建立连接。请检查安全服务中心的配置（配置路径：“系统 > 维护 > 升级中心”）、DNS的配置（配置路径：“网络 > DNS > DNS”）、物理连接和路由，确保连接到安全服务中心。
- 查看“URL过滤预定义分类查询服务过期时间”。
- 单击“激活”，激活URL过滤预定义分类查询服务。
- 在“URL分类列表”中单击“刷新”，查看最新的预定义分类。

新建URL自定义分类

新建URL分类

名称

描述 ①

选择URL对象组或者在已选框中新建URL组

可选

请输入对象组名称 查询 刷新 ② 新建

新建URL地址

匹配方式 前缀

内容 ④

确定 取消

新建URL地址组

组名 bbb

描述 bbb

③ 确定 取消

⑤ 应用 返回

HUAWEI

- 新建URL自定义分类

用户可以根据需要创建自定义URL分类，HTTP请求直接与自定义分类进行匹配，并根据自定义分类的控制动作进行URL过滤。

- 选择“UTM > Web过滤 > URL分类”。
- 单击“新建”。
- 依次输入或选择各项参数。
    - 名称:自定义分类的名称。
    - 描述:自定义分类的描述信息，方便识别自定义分类的用途。
    - 选择URL对象组:通过引用URL对象组来配置自定义分类。

      ✓将“可选”区域框中的对象组移到“已选”表示引用这些对象组。

      ✓可以在“已选”区域框中单击“新建”，创建新的对象组。

      ✓URL对象组只匹配URL的非参数部分。例如对于http://www.abcd.com/news/education.aspx?name=tom&age=20，只匹配“www.abcd.com/news/education.aspx”部分。
- 单击“应用”。

新建URL过滤器

新建URL过滤器

名称 abc

描述 abc

① ② 应用 返回

默认动作 阻断

启用URL白名单 启用URL黑名单

启用自定义分类过滤 启用预定义分类过滤 ③

控制选项	控制内容	修改
URL白名单		
URL黑名单		④

新建 ⑤ 批量修改 刷新 请输入分类名称 查询 ⑥

分类名称	描述	处理动作	配置
*aaaa	aaaa	允许	
*暴力	暴力	允许	
P2P	Web sites related to P2P	允许	

HUAWEI

URL过滤器也可以叫做URL过滤策略。配置URL过滤策略包括配置黑白名单、URL的默认访问控制动作、分类的动作和优先级。配置完成URL过滤器后，需要在Web过滤策略中引用URL过滤器。

- 新建URL过滤器
  - 选择“UTM > Web过滤 > URL过滤器”。
  - 单击“新建”。
  - 配置“名称”和“描述”。
  - 单击“应用”。
  - 在“默认动作”中配置URL过滤的默认访问控制动作。
  - 配置白名单。
  - 配置黑名单。
  - 配置自定义分类，包括是否启用自定义分类、配置自定义分类动作和优先级。
  - 配置预定义分类，包括是否启用预定义分类、配置预定义分类动作。
  - 单击“应用”。

新建Web过滤策略

Web策略列表

新建 删除 刷新 | 请输入策略名称 查询

① 名称 描述

第 1 页共 1页

新建Web过滤策略

名称 暴力

描述 ② 暴力

③ 应用 返回

URL过滤器 abc ④

启用搜索关键字过滤

⑤ 过滤选项 告警处理对象组 阻断处理对象组 修改

搜索关键字 ⑥

HUAWEI

- 新建Web过滤策略
  - 选择“UTM > Web过滤 > 策略”。
  - 单击“新建”。
  - 配置Web过滤策略的“名称”和“描述”。
  - 单击“应用”。
  - 在“URL过滤器”下拉列表框中选择URL过滤策略，引用URL过滤器。
  - 配置搜索关键字过滤。

  搜索关键字过滤指对搜索关键字进行过滤，对不符合要求的关键字进行过滤。

  目前支持进行关键字过滤的搜索引擎有Google、Yahoo、Bing、百度。
- 选中“启用搜索关键字过滤”前的复选框。
- 单击“搜索关键字”对应的 。
- 在出现的对象组列表中选择处理动作。
- 单击“确定”。

新建Web过滤策略（续）

HUAWEI

- 配置Web内容过滤。
  - 选中“启用Web内容过滤”，启用Web内容过滤功能。
  - 单击“过滤选项”中各个配置项对应的 。
  - 在出现的对象组列表中选择处理动作。
  - 单击“确定”。
- 选中/取消选中“禁止HTTP POST”，控制HTTP POST行为。
  - POST指向服务器发送包含在HTTP请求中的信息，一般用于向网页、BBS、邮件群组和数据库发送信息，例如发帖、上传网页内容等。
- 配置通过Web上传或下载的文件大小过滤。
- 单击“应用”。

应用web过滤策略

转发策略列表

①新建 删除 刷新 any zone --> any zone 查询 高级查询

ID	源地址	目的地址	用户	服务	时间段

untrust->trust

☐ IPS
☐ AV
☑ Web过滤 ②
Web过滤策略 暴力 ③
☐ 邮件过滤
☐ FTP过滤
☐ 应用控制
☐ 记录日志
☐ 开启策略会话流量统计
④ 应用 返回

  HUAWEI

- 配置完策略后，需要应用邮件过滤策略。
  - 选择“防火墙 > 安全策略 > 转发策略”。
  - 在“转发策略列表”中，单击“新建”。
  - 在“新建转发策略”区域，依次输入或选择各项参数。
  - 选中“web过滤”复选框，并选择前面配置的相应策略。
  - 单击“应用”，完成web过滤策略应用的配置。
- Web过滤URL的优先顺序为：豁免IP--› 白名单--› 黑名单--› 自定义分类和预定义分类



- Web内容过滤配置注意事项:
    - 不支持关键字的正则表达式配置
    - 非HTTP协议及非文本格式的页面内容，无法过滤
    - Web内容过滤需要进行大量解析,匹配工作，效率相对较低
    - 流量下压力下，会话会跳过检测环节直接转发
    - 虽然HTML解析过程中对确定不会显示到页面上的控制标签，属性名等不进行过滤，但某些虽然不可显示的页面字符串仍然可能会命中显示的关键字
    - 下载过程只检查TEXT/HTML和TEXT/PLAIN
    - 上传目前只检查multipart/form-data和为application/x-www-form-urlencoded,
    - 可以支持浏览器显示内容的完整过滤



总结

- WEB威胁基础知识
- URL过滤技术
- 搜索关键字过滤技术
- WEB内容过滤技术
- WEB过滤技术应用



思考题

- 判断题
  1. URL 过 滤 的 前 缀 匹配针对于hostname/path部分，参数匹配针对于query部分 。
- 多选题
  1. 下列属于WEB过滤技术的有?

  A、网站URL分类过滤

  B、恶意网页URL过滤

  C、基于内容WEB过滤

  D、基于DPI上网行为控制



习题与答案：

1、下列属于WEB过滤技术的有?

A、网站URL分类过滤

B、恶意网页URL过滤

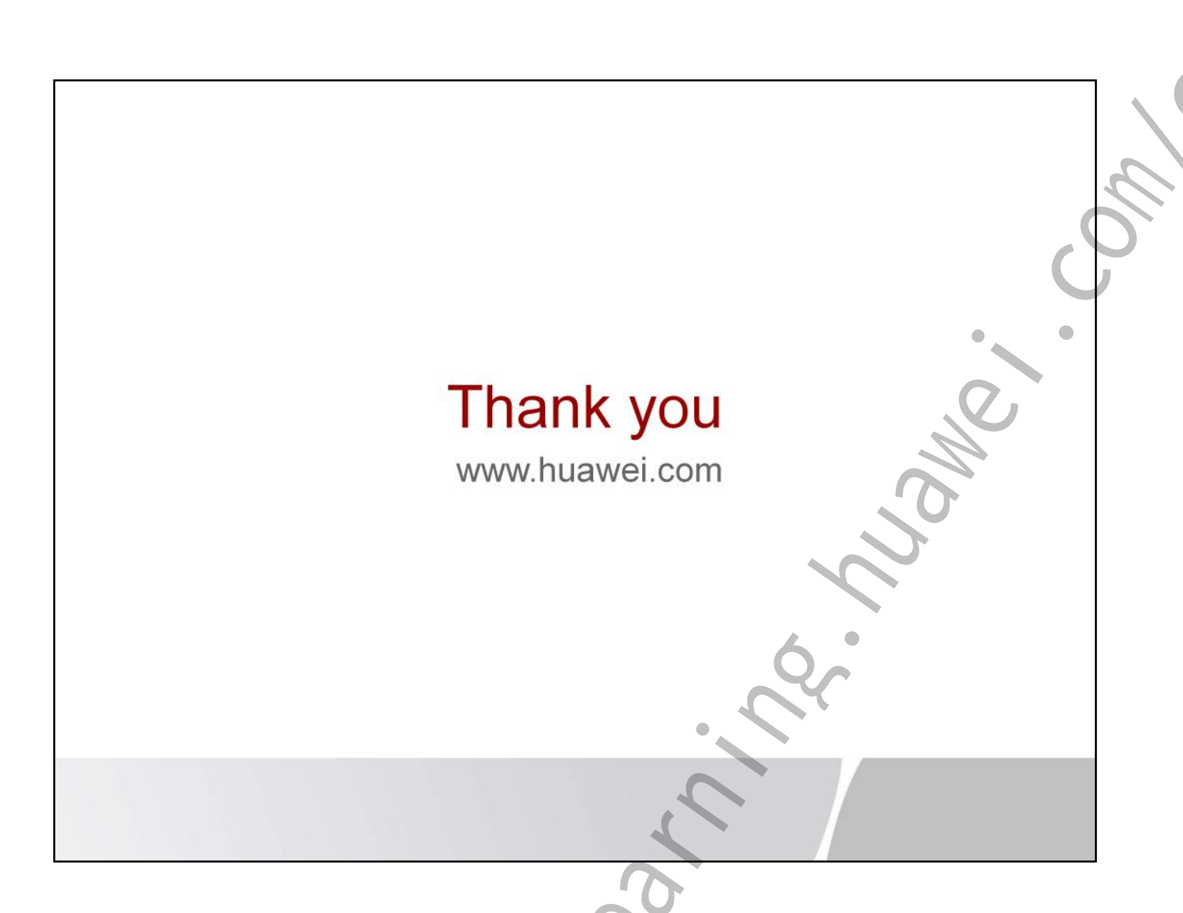
C、基于内容WEB过滤

D、基于DPI上网行为控制

答案：A | B | C

2、URL过滤的前缀匹配针对于hostname/path部分，参数匹配针对于query部分。

答案：正确


Thank you
www.huawei.com


第五章 垃圾邮件过滤
技术


HUAWEI


Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.



目标

- 学完本课程后，您将能够:
  - 了解垃圾邮件的基本概念;
  - 了解垃圾邮件的产生及危害;
  - 熟悉垃圾邮件过滤技术原理;
  - 掌握垃圾邮件过滤技术应用。





目录



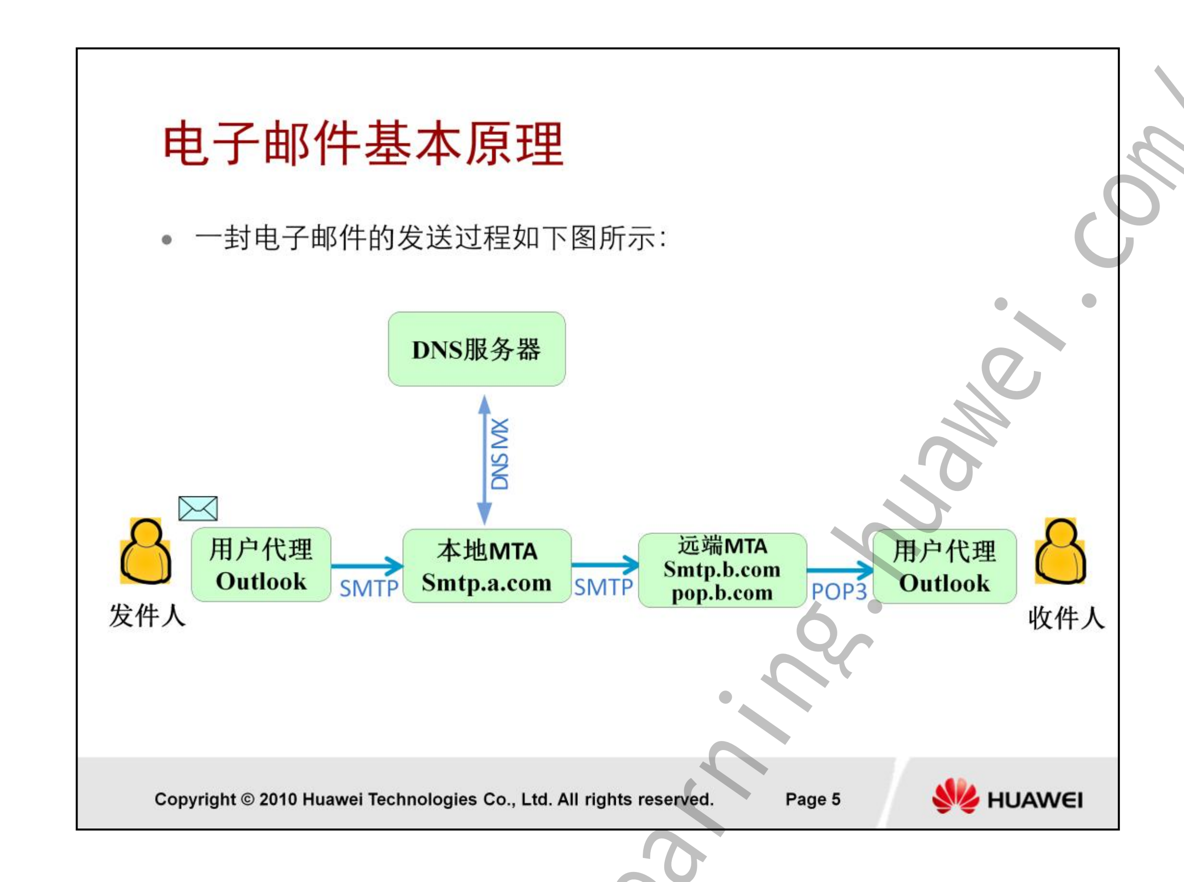
电子邮件基本概念

- 电子邮件是一种通过网络提供信息交换的通信方式。
- 完整的电子邮件一般包括邮件地址、主题、正文、附件。
  - SMTP
  - POP3
  - MUA
  - MTA

电子邮件是一种通过网络提供信息交换的通信方式。通过电子邮件，用户可以迅速地与网络上的用户发送或接受信息，这些信息可以是文字、文件、图片等。电子邮件的特点是：使用方便、传输迅速、费用低廉、易于保存、一对多发送，使得电子邮件被广泛地应用。完整的电子邮件一般包括邮件地址、主题、正文、附件。邮件地址包括收件人地址（主送人、抄送人和密送人）和发件人地址，格式一般为host@domainname.type，例如：abc@yahoo.com。 domainname为域名的标识符，也就是邮件必须要发送到的邮件目的地的域名。host为在该域名上的邮箱地址。 type一般则代表了该域名的性质或地区的代码。例如：com、edu.cn、gov、org。

- **名词解释：**
  - SMTP（Simple Mail Transfer Protocol ）是电子邮件系统的基础协议，基于TCP服务的应用层协议，端口号25，用于电子邮件的传输；
  - POP3 （ Post Office Protocol V3 ）是目前最普遍使用的邮局协议，用于把邮件从服务器（邮局）收下来；
  - MUA（Mail User Agent）邮件用户代理程序，也可以简称为用户代理程序，是指 Outlook, Foxmail 等的邮件客户端程序，实际上是这个程序在帮助用户进行邮件的发送和接收，所以称它为“代理”。
  - MTA（Mail Transfer Agent）邮件发送代理程序，一般是指邮件服务器，他们的重要职责是邮件的传递。
  - 邮箱是指在整个传递过程中，所有邮件可以被“缓存”的地方。 比如 Outlook 里面可以有本地邮箱，邮件服务器上可以有“服务器邮箱”等概念，最后收件人用 Outlook 也是通过 POP3 协议把邮件从“服务器邮箱”里接收下来。



- **一般的，一封电子邮件的发送过程如下：**
  - 发件人通过用户代理程序，如Outlook撰写邮件；
  - 该邮件通过SMTP协议传递给本地MTA（邮件传输代理）；
  - 本地MTA通过DNS服务器查询目的服务器的MX记录；
  - 本地MTA通过SMTP协议发送给远端 MTA，也就是接收端服务器；
  - 收件人使用用户代理程序，如Outlook，通过POP3协议将邮件取下来。

注意：这里提及的 DNS 服务器，和 RBL 使用的 DNS 技术没有直接联系。

DNS 服务器里有 MX 记录（邮件交换记录），简单点看，就是用于查找邮件发送路径的“邮件路由表”。 这个只是邮件发出去的时候，服务器去找接收侧服务器的地址的一个过程而已。

垃圾邮件的定义

- 垃圾邮件是包括下述属性的电子邮件：
  - 收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；
  - 收件人无法拒收的电子邮件；
  - 隐藏发件人身份、地址、标题等信息的电子邮件；
  - 含有虚假的信息源、发件人、路由等信息的电子邮件。

携带病毒和木马的邮件也是垃圾邮件！



简单来说：垃圾邮件就是为实现某种目的，而批量发送未经过收件人同意的电子邮件。

在该规范中并未将病毒邮件列入其中，但在现实网络中以传播病毒和木马为目的的电子邮件在垃圾邮件中所占比例成上升趋势。

垃圾邮件产生原因

- 经济利益的驱动；
- SMTP协议缺陷；
- 开放的互联网；
- 无意导致的误发送。



1985年8月出现了第一封通过电子邮件发送的连锁信，这是由记录的最早的垃圾邮件。1994年4月出现了通过电子邮件发送的广告邮件，该邮件发送范围之广导致在互联网上产生严重影响，并首次以SPAM命名垃圾邮件。1995年5月专门用于发送垃圾邮件的群发软件Floodgate出现。

- 技术环境：互联网发展初期的局限性导致对协议安全的忽略。
  - SMTP 协议非常开放，早期甚至连起码的双向认证都没有，这为垃圾邮件的产生做了技术的铺垫。
  - SMTP缺乏对发信方进行身份验证机制；
  - 协议基于文本方式，无加密校验机制；
  - 邮件可通过第三方转发。
- 经济利益或者其他利益驱动
  - 大量的广告、网络营销：这是最传统的，相对危害较小，但是很让人烦。
  - 非法言论：不利于社会安定、国家安全；
  - 钓鱼（含恶意软件）：信息安全，损坏信息资产，影响设备正常工作。

最近一次垃圾邮件报告显示，垃圾邮件甚至已经用于操纵股市的股票，通过大量垃圾邮件诽谤、造谣，制造舆论控制某一支股票的涨跌，从而牟利。

- TCP/IP协议的开放性

垃圾邮件的发送手段

- 通过各种方法（购买，偷窃）获取接收人列表
- 使用专门的服务器来发送垃圾邮件
- 通过破解等黑客手段挟持他人服务器或者主机来发送垃圾邮件
- 破解他人的社交网络帐号来发送垃圾邮件
- 综合运用多种躲避垃圾邮件检查的手段



曾经有过很多臭名昭著的垃圾邮件服务器，但是在塞班斯法案执行后，专用于发送垃圾邮件的服务器逐渐减少，但是仍旧是不可忽视的力量。

塞班斯法案是信息安全领域很重要的一个法案，对于信息监管提出了很严厉的要求。

互联网垃圾邮件现状

- 垃圾邮件占总邮件数量的比例大约在 80% - 90%。
- 垃圾邮件占用了大量的网络资源和存储空间
- 垃圾邮件浪费了邮件使用者的宝贵时间
- 由于钓鱼等行为的存在，垃圾邮件严重影响了信息安全。





垃圾邮件已经成为互联网最突出的问题之一，根据赛门铁克的统计，全球互联网上每天垃圾邮件的发送量在几百亿甚至上千亿封。垃圾邮件占总邮件量的比例大约在 80% - 90%。

目前存在不少来自其他国家或者反动组织发送的政治言论类电子邮件，这就跟垃圾的商业广告一样，销售和贩卖他们的所谓言论。

蠕虫病毒邮件。越来越多的病毒通过电子邮件来迅速传播，这也的确是一条迅速而且有效的传播途径。

恶意邮件（恐吓、欺骗性邮件）。比如phishing，这是一种假冒网页的电子邮件，完全是一种诡计，来蒙骗用户的个人信息、账号甚至信用卡。

以木马和病毒、低俗内容以及垃圾邮件为代表的影响纯净网络建设的三大因素，不仅影响到互联网信息的甄别和获取，还严重威胁着各个国家的网络安全。

垃圾邮件的危害

- 降低生产力
- 被黑客利用
- 损害ISP品牌形象
- 危害社会



- 降低生产力

泛滥成灾的商业性垃圾信件每五个月数量翻倍，阅读、删除这些垃圾邮件都会带来生产力的损失。

- 被黑客利用

垃圾邮件被黑客利用成助纣为虐的工具，黑客在垃圾邮件中携带木马、 病毒并诱惑用户去执行，从而在用户主机上植入木马、病毒程序。

- 损害ISP品牌形象

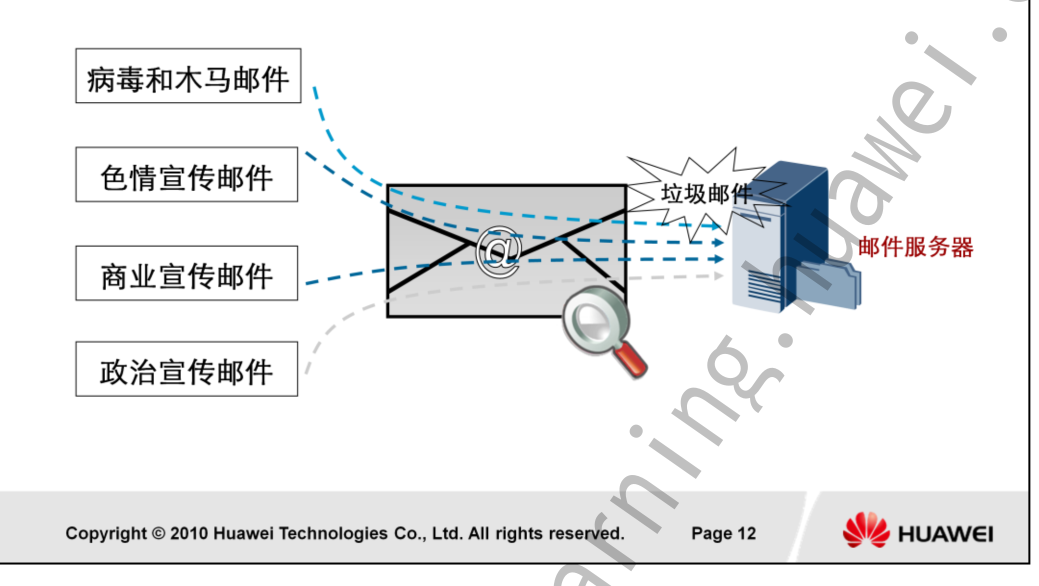
频繁转发垃圾邮件的ISP主机会被上级国际因特网服务提供商列入国际垃圾邮件数据库，从而导致该主机发出的邮件被其它ISP拒绝。

- 危害社会

妖言惑众、骗人钱财、传播色情等内容的垃圾邮件，将危害现实社会。

垃圾邮件主要类型

- 在这些类型的垃圾邮件中，目前尤以病毒邮件居多，高达40%以上。



垃圾邮件技术分析

动态IP	动态内容	分布式发送	结合病毒特性
垃圾邮件多采用IP地址或域名变换技术，达到欺骗反垃圾邮件系统的目的。	关键字动态变化 采用附件代替文本内容 信头、正文动态变化 内容图片化	采用分布式的发送方式，以防止地址或域名屏蔽。	结合蠕虫病毒的自动传播机制，实现垃圾邮件的大量发送。



技术的进步及普及导致垃圾邮件的制作者的技术水平越来越高，对新技术的熟练使用使垃圾邮件的检测难度增大。垃圾邮件采用多种动态变换技术逃避检测。针对目前反垃圾邮件技术手段，垃圾邮件通常采用以下技术逃避检测：动态IP、动态内容、分布式发送、结合病毒特性。



目录



常见的垃圾邮件过滤技术

统计法	列表法	源头法	其它
贝叶斯	静态黑名单	SenderID	内容过滤
带宽/连接限制	静态白名单	Domainkeys	图片识别技术
邮件数量限制	RBL	SPF	意图分析技术
信誉评级			



垃圾邮件过滤技术——统计法

- 贝叶斯算法
  - 基于统计方法，采用标记权重的方式，根据对已知的垃圾邮件和非垃圾邮件为样本进行的内容分析和统计来计算下一封邮件为垃圾邮件的概率，生成过滤规则；
- 连接/带宽统计
  - 通过统计单位时间内某固定IP地址试图连接的数量是否在预定范围，或限制有效带宽实现反垃圾邮件。
- 邮件数量限制
  - 限制单个IP在单位时间内可发送的邮件数量。
- 信誉评分技术
  - 基于统计的技术，采用信誉评级的方法实现邮件等级定义。



采集垃圾邮件样本通常的办法是使用蜜罐邮箱。

由于贝叶斯算法是通过垃圾邮件样本学习实现的过滤，因此获得的垃圾邮件样本越多则效果越好。

信誉评分技术：可以电子邮件信誉比喻成信用纪录。如果信用纪录不良，你就无法从银行取得优惠的贷款利息。同理，如果电子邮件信誉差，发出的电子邮件就会被归入垃圾邮件。

垃圾邮件过滤技术——列表法

- DNS-RBLs技术
  - 通过域名反向解析检查所收到邮件的IP地址与其名称是否一致， 该技术对于使用虚假IP发送的垃圾邮件有较好的过滤效果。
- 静态黑名单
  - 通过配置静态黑名单对垃圾邮件进行过滤，但该方法对于IP地址、域名变换技术并无效果，因此在实际网络中并未采用。
- 静态白名单
  - 通过设置可信名单的方式实现，同样有静态黑名单方法的问题。



RBL原理：SMTP服务器接收到链接请求， 对链接地址进行DNS反向查询， 与RBL服务器建立查询， 查询得到肯定的结果，则拒绝该连接。 查询无结果，继续进行连接。

RBL的优点在于RBL服务提供商维护公共RBLs，使用者仅需订阅实时黑名单服务。而且RBLs对于网络开销非常低。RBLs缺点在于易于产生误报。因此在使用中需谨慎使用丢弃原则。

垃圾邮件过滤技术——源头法

- SenderID
  - 该方案为Microsoft提出，并得到多数网络厂商支持，但并未通过 IETF。该技术完全依赖于DNS特性，因此容易遭受攻击。
- SPF技术
  - SPF 是发送方策略框架 (Sender Policy Framework) 的缩写，其 目的用于防止伪造邮件地址 。
- Domainkeys
  - 采用验证邮件发件人是否与其声称的邮件域一致，并验证邮件的 完整性。该技术为一种公钥+私钥的签名技术。

 Page 18



SPF基于反向查询技术判断邮件的指定域名和IP地址是否是完全对应的。基本原理就是伪造邮件的地址是不会真实来自RMX地址，因此可以判断是否伪造。

垃圾邮件过滤技术——其他

- 多重图片识别技术
  - 识别通过图片进行隐藏的垃圾邮件。
- 意图分析技术
  - 邮件动机分析技术。
- 内容过滤
  - 通过分析邮件的内容采用关键字过滤方法。



大部分垃圾邮件背后的动机是使收信方响应其目的接受某物，例如购买商品、登陆某网站我们把这些动机被称为邮件“意图”，通过分析邮件的这些特点防御垃圾邮件的技术称为意图分析。



目录

1. 垃圾邮件介绍
2. 垃圾邮件过滤技术介绍
3. **RBL邮件过滤技术**
4. 邮件内容过滤技术
5. 垃圾邮件过滤技术应用



RBL邮件过滤

- RBL（Real-time Blackhole List），即反垃圾邮件
- RBL通过定义一个黑名单列表，在该列表中的IP地址对外发布的邮件即为垃圾邮件。
- 提供RBL服务的机构会实时更新黑名单列表来保证可以过滤最新的垃圾邮件。
- RBL过滤只支持对SMTP协议传输的邮件进行过滤。

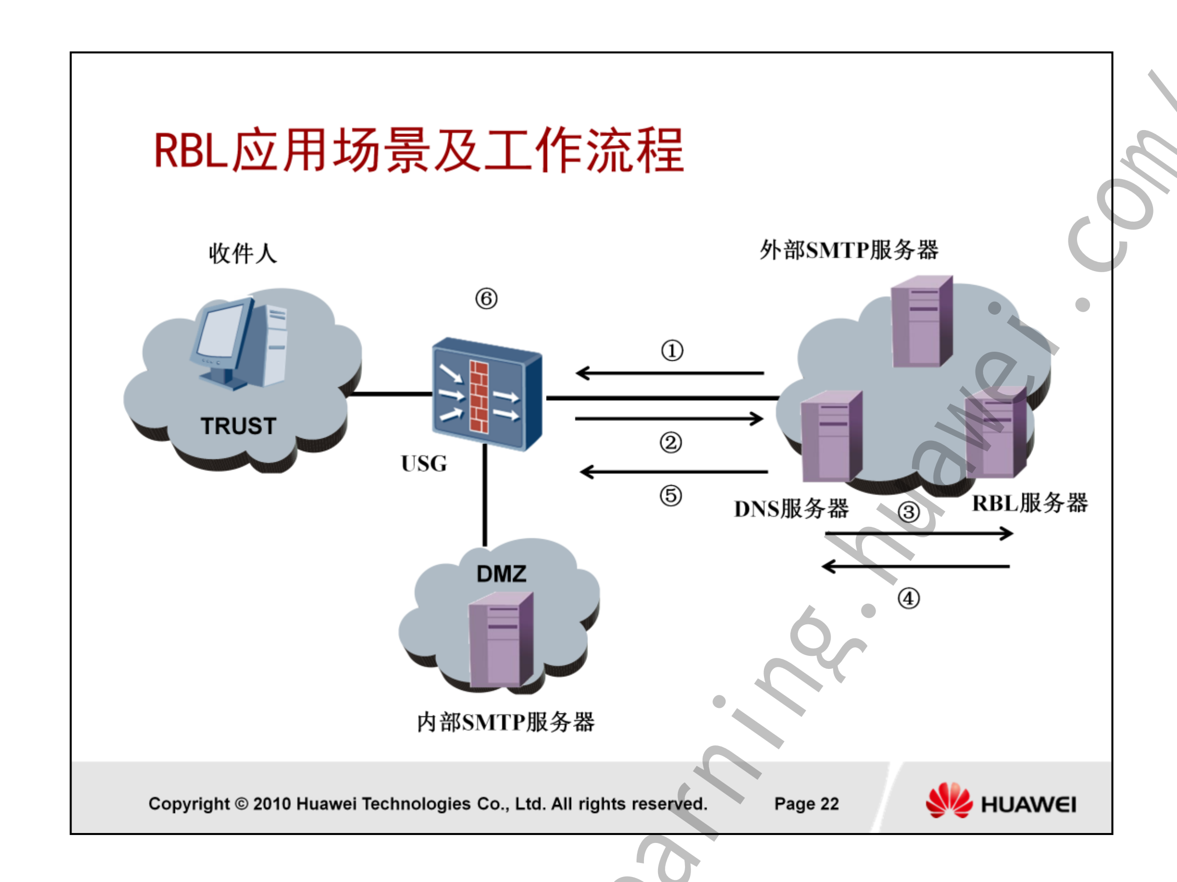


RBL（Real-time Blackhole List）过滤功能可以通过本地和远程黑白名单对使用SMTP协议传输的邮件进行检查，有效阻隔垃圾邮件，保护邮件服务器。

设备检测到SMTP连接请求后，提取SMTP连接的源IP地址，与第三方组织提供的动态更新的远程实时黑名单以及本地黑白名单进行比对，对列入黑名单的邮件进行阻断。

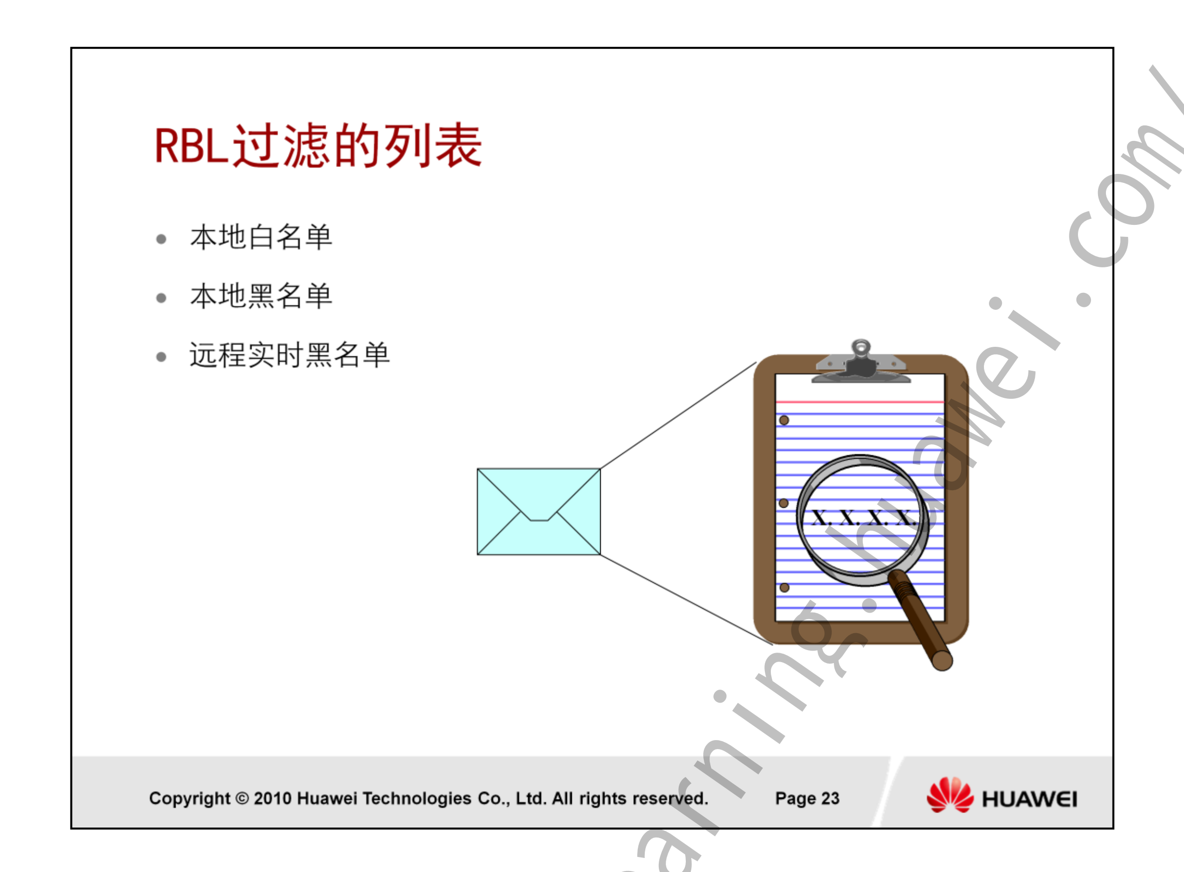
RBL过滤技术是在邮件发送邮件数据之前进行过滤，及时有效的阻断了垃圾邮件，节约邮件服务器资源。在邮件对话SMTP连接开始阶段，检查客户端IP地址是不是特定的不允许连接的地址，如被列入黑名单IP就会被立刻拒绝连接。这里的黑名单可以是实时黑名单（RBL），也可以是用户配置的黑名单列表。

RBL过滤技术实际上是一个可供查询的IP地址列表，通过DNS的查询方式来查找一个IP地址是否存在于该地址列表，来判断其是否被列入了该实时黑名单中。



- RBL工作流程:
  - 外部邮件服务器向内网发送SMTP请求;
  - USG收到SMTP请求后，提取SMTP连接的源IP地址并将查询集合和提取的源IP地址发送给DNS服务器;
  - DNS服务器根据查询集合向RBL服务器转发RBL查询请求;
  - RBL服务器以应答码的形式将查询结果返回给DNS服务器;
  - DNS服务器向USG转发应答码;
  - USG根据应答码判断该SMTP连接的邮件是否为垃圾邮件，并进行相应处理。

如果RBl服务器回复的应答码和USG上配置的应答码一致，该SMTP邮件将被视为垃圾邮件；如果RBL服务器回复的应答码和USG上配置的应答码不一致，该SMTP邮件将被放行



- 本地白名单

当某个邮件的源地址命中了本地白名单，那么本地黑名单和远程黑名单不再对此源IP地址进行匹配，该邮件被直接转发。白名单的设置有利于提高匹配效率。

- 本地黑名单

本地黑名单的优先级比远程黑名单高，当某个邮件的源地址命中了本地黑名单，那么远程黑名单不再对此源IP地址进行匹配，该邮件直接阻断。

RBL过滤依赖于远程黑名单的完整性，当远程黑名单不包含SMTP请求的源IP地址时，无法过滤该邮件。此时，可以通过补充本地RBL黑名单来完成过滤。

- 远程实时黑名单

远程实时黑名单是由第三方组织提供的动态更新的黑名单。第三方组织实时更新和维护RBL并通过RBL服务器提供查询服务。

RBL过滤的响应方式

- 告警（Alert）
  - 正常转发邮件，并发出日志告警信息。
- 阻断（Block）
  - 阻断邮件，并发出日志告警信息。





目录

1. 垃圾邮件介绍
2. 垃圾邮件过滤技术介绍
3. RBL邮件过滤技术
4. **邮件内容过滤技术**
5. 垃圾邮件过滤技术应用



邮件内容过滤带来的价值

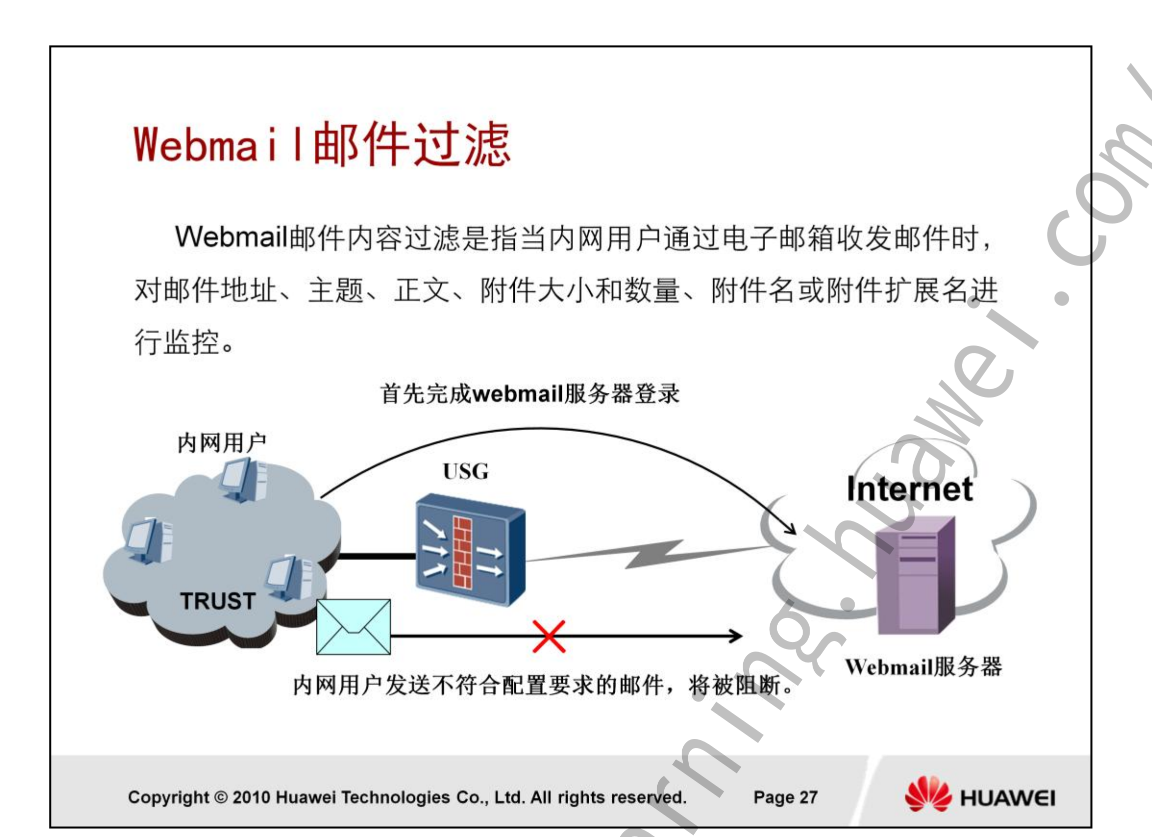
邮件内容过滤特性从邮件中提取邮件要素并对其进行过滤，消除其带来的内容安全威胁，给用户带来如下价值：

- 防信息泄露
- 屏蔽敏感信息和反动言论
- 收发邮件权限控制
- 防带宽过度占用



当内网用户通过Webmail或SMTP/POP3客户端收发电子邮件时，邮件内容过滤对邮件地址、主题（标题）、正文、附件大小和数量、附件名或附件扩展名等进行监控，防止数据泄漏或敏感信息传输。

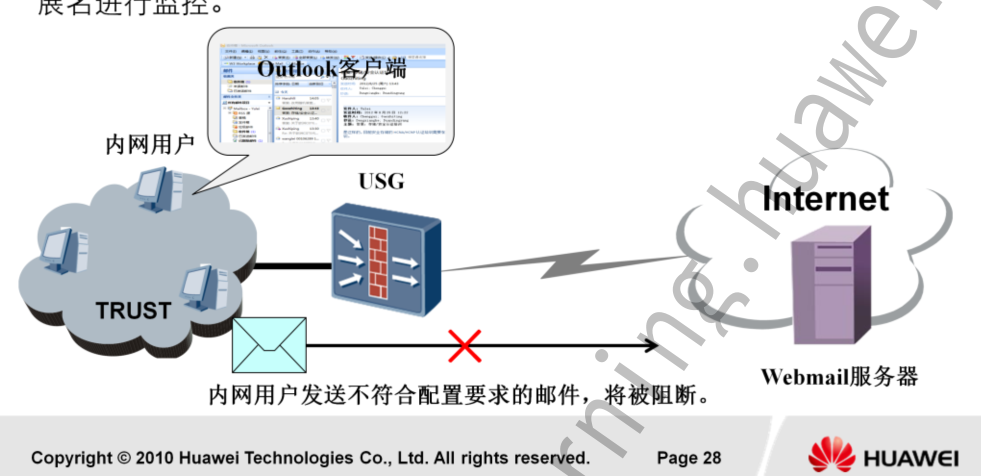
- 邮件内容过滤带来的价值：
  - 防信息泄露，通过邮件内容过滤防止内网用户使用SMTP邮件或Webmail将内网机密/敏感信息泄露到外部网络。
  - 屏蔽敏感信息和反动言论，通过邮件内容过滤防止内网用户使用POP3从外网接受敏感信息或反动言论。
  - 收发邮件权限控制，通过邮件地址过滤控制邮件使用者的收发权限。
  - 防带宽过度占用，控制附件大小防止超大附件过度占用网络带宽。



Webmail是指利用网络浏览器来收发电子邮件的服务或技术。Webmail不需要借助邮件客户端来收发邮件，只要能上网、有Webmail的账号就能通过使用网络浏览器从邮件服务器（电子邮箱）上收发邮件，极大地方便了用户。

Webmail根据签名文件从http Webmail流量提取邮件要素(包括收件人、发件人、主题、正文、附件文件名、附件文件类型、附件大小)，再根据邮件策略中的配置对提取到的邮件要素进行过滤，最终将过滤结果以日志方式通过管理员，并阻断违规的http Webmail流量。

注：Webmail过滤不支持内网用户收邮件的过滤。



SMTP（Simple Mail Transfer Protocol）主要负责在Internet上对电子邮件进行传输。POP3（Post Office Protocol）允许客户端从邮件服务器上取得邮件。

通过SMTP/POP3传输的邮件需要在用户PC上安装一个客户端，常见的有Outlook和Foxmail。

SMTP/POP3邮件内容过滤是指当内网用户通过邮件客户端收发邮件时，对邮件地址、标题、正文、附件大小和数量、附件名或附件扩展名进行监控。

SMTP/POP3邮件过滤采用全代理方式，收取并解析提取邮件的各项要素(包括收件人、发件人、主题、正文、附件文件名、附件文件类型、附件数目、附件大小），然后根据邮件策略中的配置进行过滤，最终将过滤的结果分别采用日志和宣告的方式通知管理员和邮件使用者。

邮件内容过滤方式

过滤配置项	匹配方式	引用的公共模式组类型
收件人或发件人 邮件地址	前缀/后缀/任意/精确	邮件地址
邮件主题 邮件正文 附件名	任意	关键字
附件扩展名 （文件扩展名）	精确	文件扩展名
附件大小	直接配置，不引用公共模式组	-
附件数量	直接配置，不引用公共模式组	-

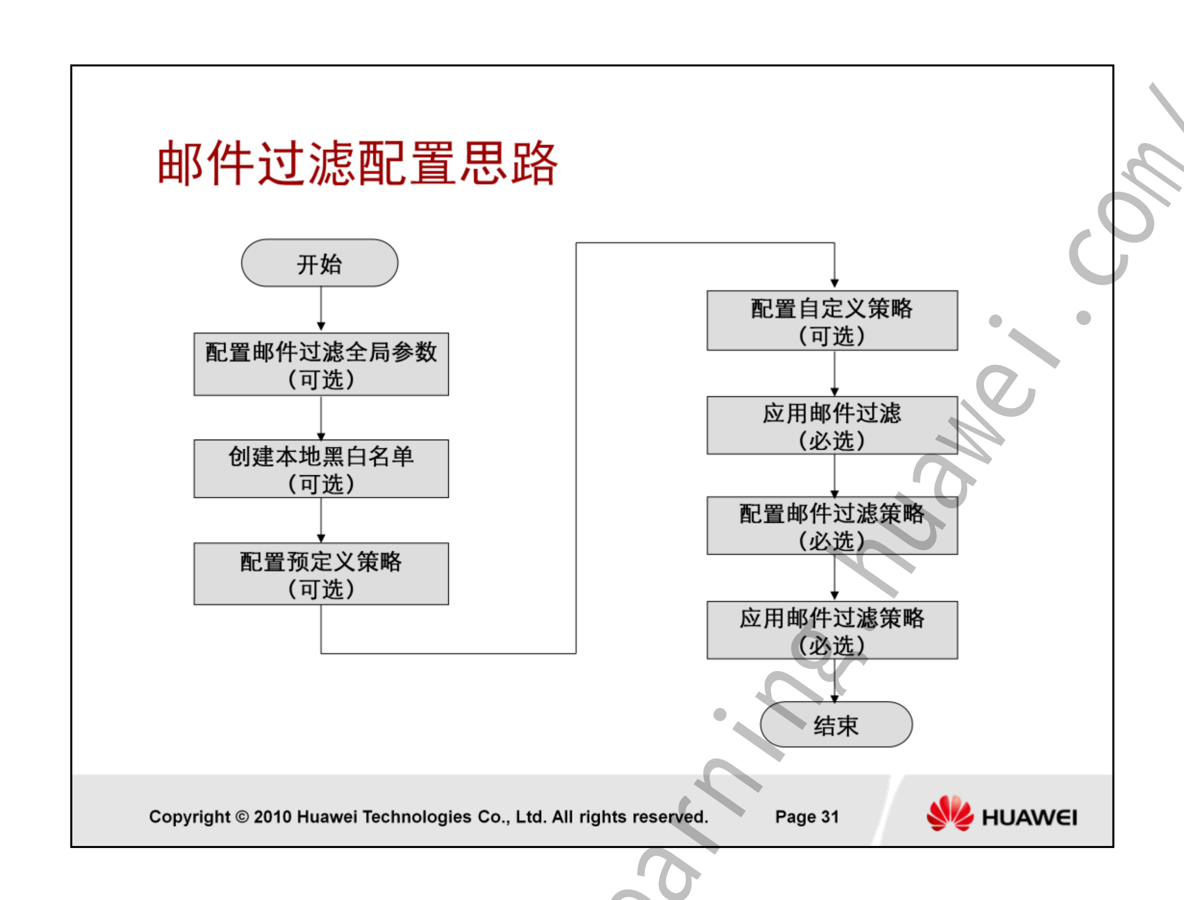


SMTP/POP3的邮件与附件作为一个整体进行发送和接收，如果附件不符合设备的策略要求，整封邮件会被阻断；与SMTP/POP3不同，Webmail的附件上传与邮件发送是两个相对独立的操作，对于Webmail附件上传行为，如果附件不符合设备的策略要求，会对当前附件上传行为进行阻断，但不影响符合策略要求的邮件正文发送。



目录





- 配置垃圾邮件过滤全局参数

　　当需要在邮件过滤策略中引用垃圾邮件过滤时需要配置，内容包括： 垃圾邮件过滤功能全局开关、本地黑白名单使能开关、查询垃圾邮件服务器的DNS地址。

- 创建本地黑白名单:

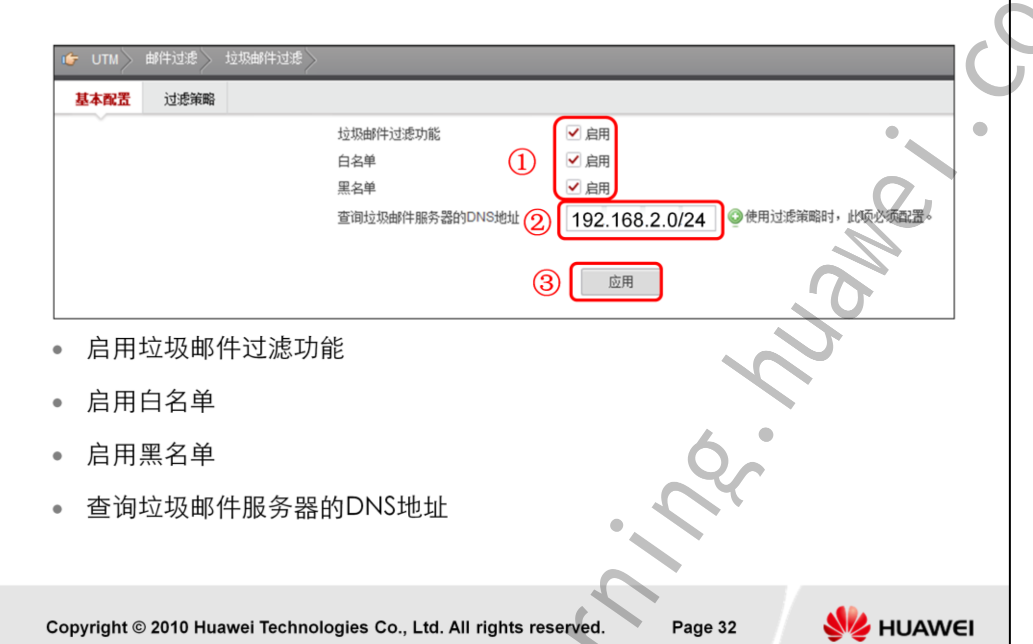
　　当需要在垃圾邮件过滤中使用本地黑名单时需要配置。

- 配置预定义策略

　　如果需要使用系统预置的Symantec服务器作为RBL服务器进行RBL远程查询，需要配置预定义策略。

- 配置自定义策略

　　如果需要使用自定义的服务器作为RBL服务器进行RBL远程查询，请配置自定义策略。



- 选择“UTM > 邮件过滤 > 垃圾邮件过滤”。
- 选择“基本配置”页签。
- 选中“垃圾邮件过滤功能”对应的“启用”复选框。
- 选中“白名单”对应的“启用”复选框。（可选）
- 选中“黑名单”对应的“启用”复选框。（可选）
- 在“查询垃圾邮件服务器的DNS地址”中输入用于查询RBL的DNS服务器地址。
  - DNS服务器用来查找RBL服务器，只有配置了用于查询RBL的DNS服务器后，设备才能与RBL服务器建立连接。可以通过点击右边的添加DNS服务器地址。
- 单击“应用”。
- 在弹出的提示框中单击“确定”。

创建本地白名单

- 点击新建白名单
- 输入符合白名单列表的IP地址及掩码

- 选择“UTM > 邮件过滤 > 垃圾邮件过滤”。
- 选择“基本配置”页签。
- 在“白名单列表”区域框中，单击“新建”。
- 输入IP地址/掩码。
  - IP地址/掩码可用以下格式：IP地址/子网掩码：例如192.168.1.0/24
  - IP地址/掩码长度：例如192.168.1.0/24。
  - IP地址\反向子网掩码：例如192.168.1.0\0.0.0.255。
  - IP地址\反向掩码长度：例如192.168.1.0\8。
- 单击“确定”。
- 重复执行上述操作，可继续添加本地白名单。



- 选择“UTM > 邮件过滤 > 垃圾邮件过滤”。
- 选择“基本配置”页签。
- 在“黑名单列表”区域框中，单击“新建”。
- 输入IP地址/掩码。IP地址/掩码可用以下格式：
  - IP地址/子网掩码：例如192.168.1.0/255.255.255.0。
  - IP地址/掩码长度：例如192.168.1.0/24。
  - IP地址\反向子网掩码：例如192.168.1.0\0.0.0.255。
  - IP地址\反向掩码长度：例如192.168.1.0\8。
- 单击“确定”。
- 重复执行上述操作，可继续添加本地黑名单。



- 选择“UTM > 邮件过滤 > 垃圾邮件过滤”。
- 选择“过滤策略”页签。
- 单击“预定义策略”对应的配置按钮。
- 配置相关参数：动作为告警或阻断、策略启用。
- 单击“应用”。



- 选择“UTM > 邮件过滤 > 垃圾邮件过滤”。
- 选择“过滤策略”页签。
- 单击“新建”。
- 配置自定义策略的“名称”和“描述”。
- 单击“应用”后继续配置自定义策略参数。

配置自定义策略（续）

- 垃圾邮件服务器查询集合： RBL请求的查询集合用来定位RBL服务器。
- 应答码：设备将匹配到应答码的邮件作为垃圾邮件进行过滤。

- 配置垃圾邮件服务器查询集合。
  - RBL请求的查询集合用来定位RBL服务器。查询集合由RBL服务提供商提供。一个策略只能配置一个查询集合。例如：rbl.anti-mail.com.cn。
- 配置邮件匹配策略后设备采取的动作。
- 配置应答码列表，单击“新建”。
- 配置垃圾邮件应答码
  - 任意应答码：选中表示对任意应答码都进行匹配。
  - 应答码：设备将匹配到应答码的邮件作为垃圾邮件进行过滤。如果RBL服务器不回复应答码或回复的应答码与设备侧配置的应答码不一致时，放行邮件。
  - 应答码会因为RBL服务提供商的不同而不一样，具体请咨询RBL服务提供商。

注意：“应答码”与“任意应答码”互斥，只能配置其中一个。

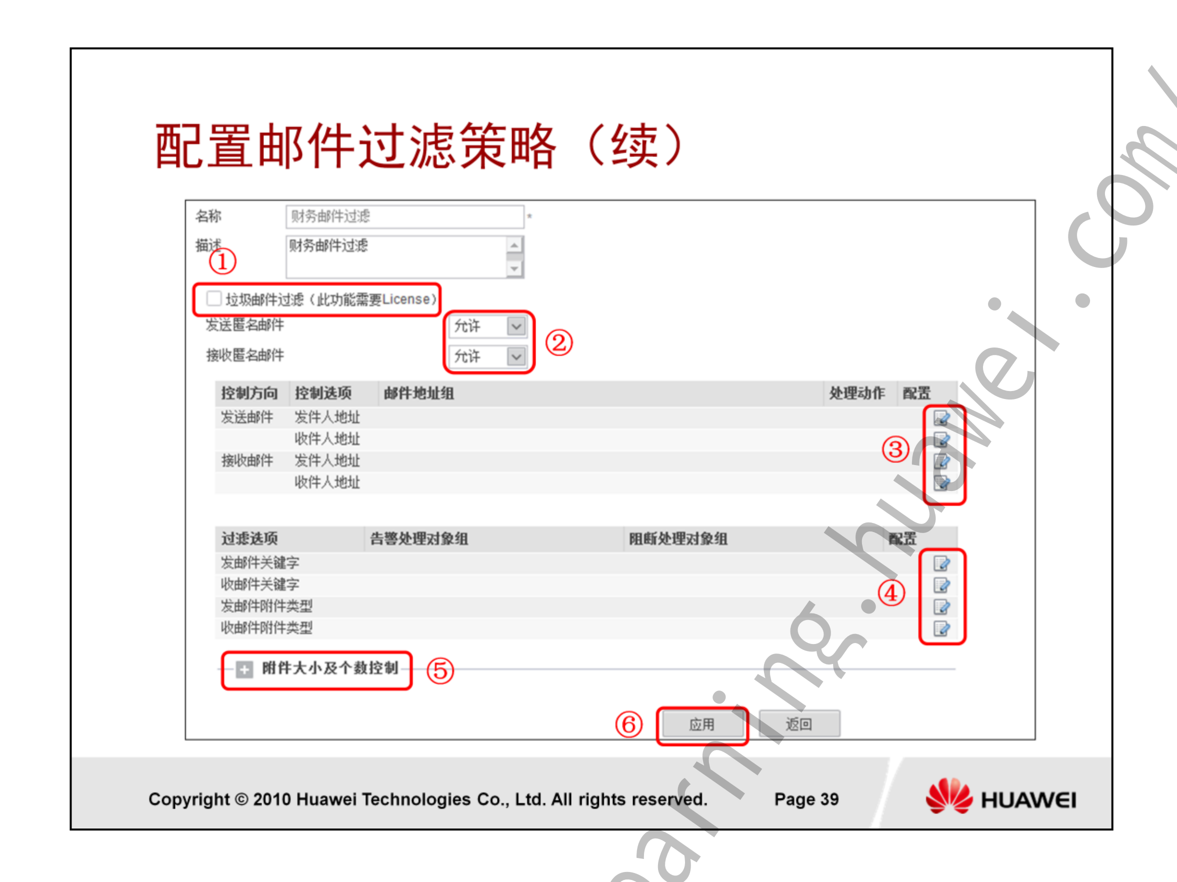
- 单击“确定”。
- 单击“应用”。
- 在弹出的提示框中单击“确定”。

配置邮件过滤策略



- 启用邮件过滤
- 配置邮件过滤策略

- 选择“UTM > 邮件过滤 > 策略”。
- 选中“邮件过滤”对应的“启用”复选框。
- 单击“应用”。
- 在弹出的提示框中单击“确认”。
- 选择“UTM > 邮件过滤 > 策略”。
- 单击“新建”。
- 配置邮件过滤策略的“名称”和“描述”。
- 单击“应用”，继续邮件过滤策略配置。



- 选中“垃圾邮件过滤”前的复选框，启用RBL过滤。 此功能需要用户购买的License中支持RBL过滤。
- 在“发送匿名邮件”和“接收匿名邮件”中选择过滤动作。
- 配置邮件地址（收件人、发件人）过滤，单击“发送邮件”或“接收邮件”中收发件人对应的 。
- 配置邮件主题、正文过滤和附件类型过滤，单击“发邮件关键字”、“收邮件关键字”、“发邮件附件类型”或者“收邮件附件类型”对应的 。
- 配置附件个数和附件大小过滤。
- 单击“应用”，完成邮件过滤策略配置。



- 选择处理动作。
  - 选择“允许”，邮件地址匹配“已选”区域框的对象组时，设备放行该邮件，并阻断未匹配对象组的邮件。
  - 选择“阻断”，邮件地址匹配“已选”区域框的对象组时，设备阻断该邮件，并放行未匹配对象组的邮件。
- 在“可选”区域框中选择要引用的对象组，单击 ，将对象组移到“已选”区域框中。如果没有已有地址组，可以直接点击已选框中的“新建”，建立邮件地址组。
  - 配置“组名”
  - 在邮件地址列表中选择“新建”
  - 在新建Email地址中选择“匹配方式”，匹配方式有：前缀、后缀、精确、关键字
  - 在新建Email地址内容中输入相应参数
  - 单击两次“确定”完成地址组配置
- 单击“确定”，完成邮件地址过滤配置。

配置邮件主题、正文过滤和附件类型过滤

邮件关键字配置

② 新建 请输入

对象组名称

全部关键字组

search

download

新建关键字组

名称 ③ abc *

描述

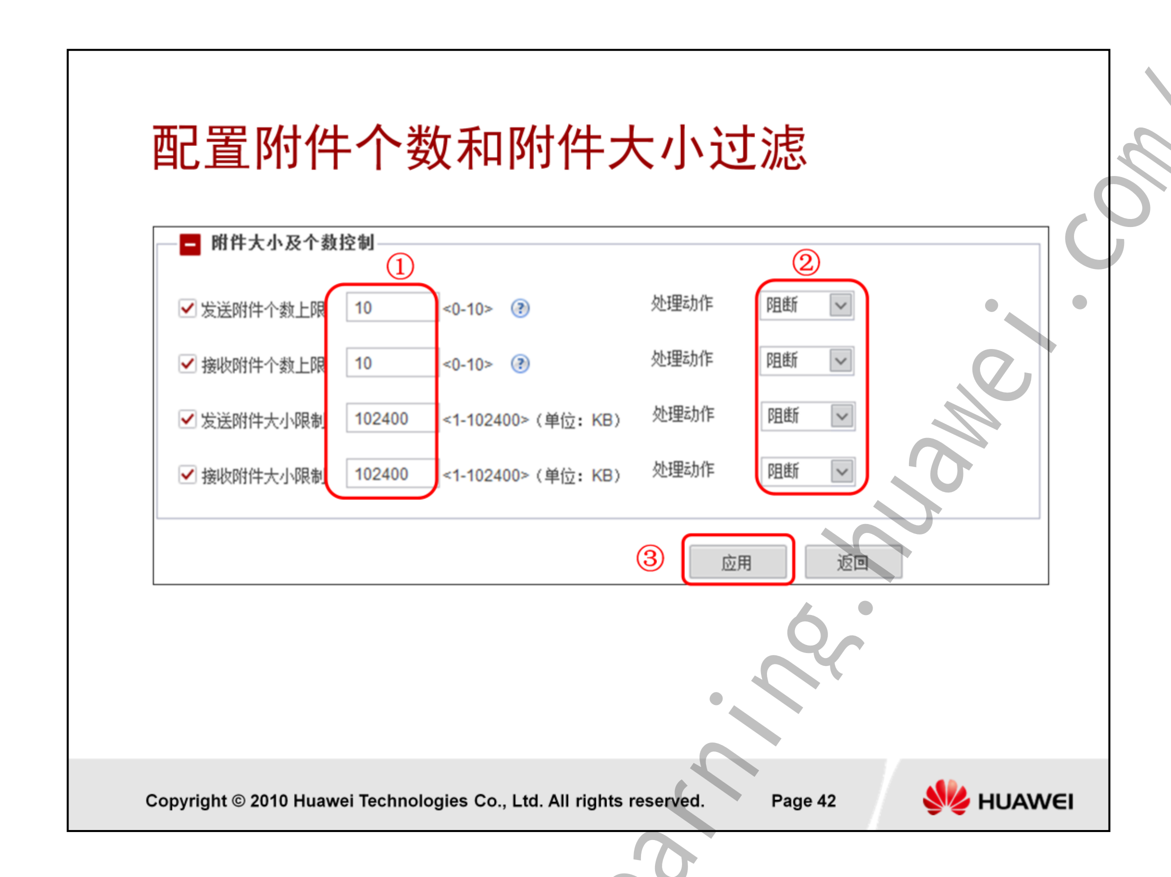
关键字 ④ 色情

每个关键字的长度为2~127个字符，行首或行尾处的空白字符，如空格、制表符等不计长度；
回车开始输入新的关键字，例如：
暴力
成人

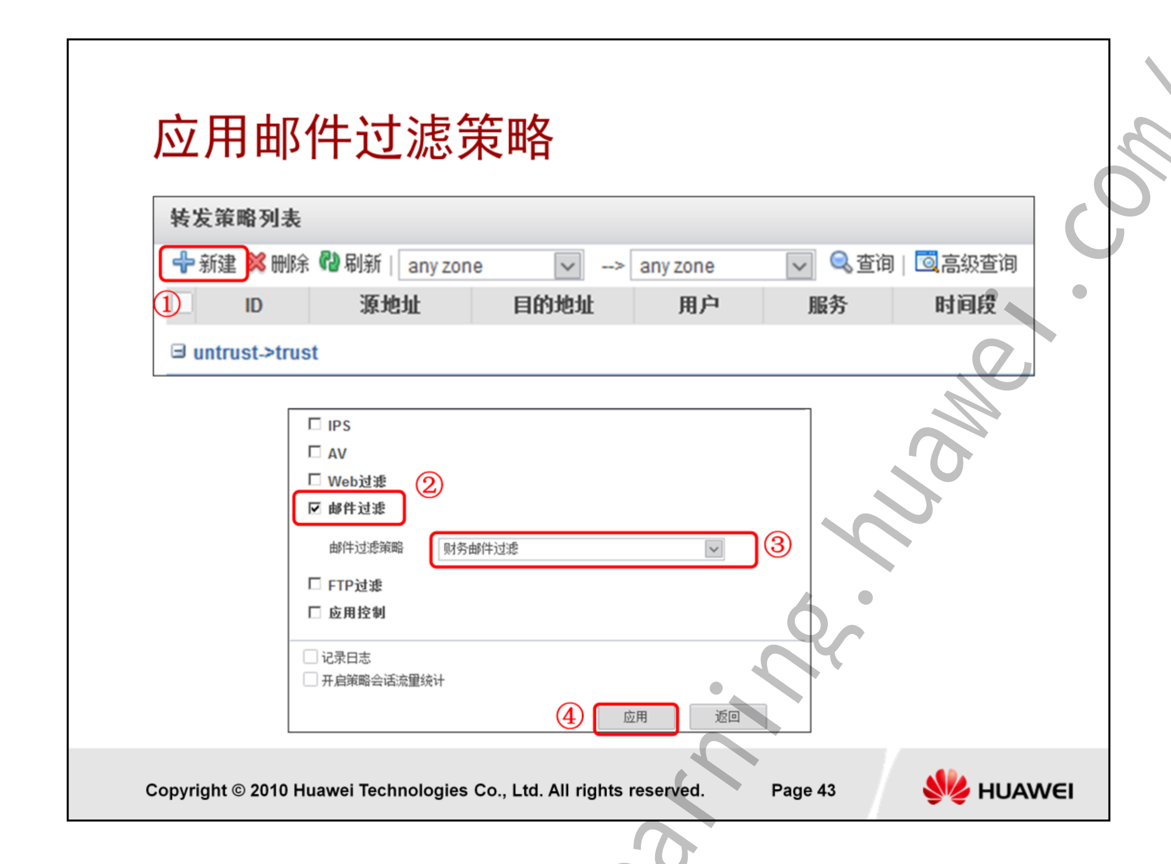
⑤ 确定 取消

⑥ 确定 取消

- 在出现的对象组列表中选择处理动作。处理动作包括：不处理、告警、阻断
- 如果没有已有对象组或对象组不满足邮件过滤条件，可以直接点击邮件关键字配置中的“新建”，建立新关键字组。
  - 单击“新建”
  - 在新建关键字组中，输入名称
  - 在关键字中输入需要邮件过滤的关键字
  - 单击“确定”
- 单击“确定”，完成邮件主题、正文、附件过滤配置。



- 勾选“发送附件个数上限”、“接收附件个数上限”、“发送附件大小限制”或“接收附件大小限制”，输入数值。
- 在“处理动作”中选择处理动作。



- 选择“防火墙 > 安全策略 > 转发策略”。
- 在“转发策略列表”中，单击“新建”。
- 在“新建转发策略”区域，依次输入或选择各项参数。
- 选中“邮件过滤”复选框，选择前面配置的相应邮件过滤策略。
- 单击“应用”，完成邮件过滤策略应用的配置。



总结

- 垃圾邮件的基本概念；
- 垃圾邮件的产生及危害；
- 垃圾邮件过滤技术原理；
- 垃圾邮件过滤技术应用。



思考题

- 单选题

  1. 下列反垃圾邮件技术中，属于采用统计方法的是?

  A、贝叶斯　B、静态黑名单　C、RBL　D、内容过滤

- 判断题

  1. USG根据应答码判断该SMTP连接的邮件是否为垃圾邮件，并进行相应处理。 如果RBl服务器回复的应答码和USG上配置的应答码不一致，该SMTP邮件将被视为垃圾邮件。 如果RBL服务器回复的应答码和USG上配置的应答码一致，该SMTP邮件将被放行。



习题与答案：

1、下列反垃圾邮件技术中，属于采用统计方法的是?

A、贝叶斯

B、静态黑名单

C、RBL

D、内容过滤

答案：A

2、USG根据应答码判断该SMTP连接的邮件是否为垃圾邮件，并进行相应处理。 如果RBl服务器回复的应答码和USG上配置的应答码不一致，该SMTP邮件将被视为垃圾邮件。 如果RBL服务器回复的应答码和USG上配置的应答码一致，该SMTP邮件将被放行。

答案：错误

Thank you

www.huawei.com


第六章
应用控制
www.huawei.com
HUAWEI
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.



目标

- 学完本课程后，您将能够:
  - 了解SA（Service Awareness）产生背景;
  - 掌握应用控制各种技术工作原理;
  - 掌握应用控制技术的应用。





目录





互联网现状及发展趋势

- 网络用户规模呈几何级数增长
- 网络应用种类日益扩展
- 网络带宽需求不断扩大



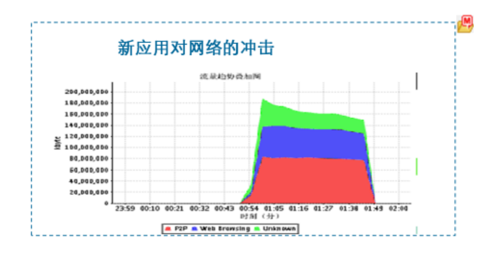


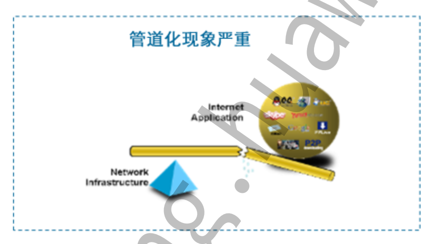
Internet发展的几十年来，网络用户数、网络应用种类、网络带宽都呈现出爆炸式的增长，对社会和人们的生活产生了巨大的影响。网络的功能，从最初的互连互通为主，到后来的以Email、WWW浏览、FTP下载等信息共享为主，到今天的P2P、VoIP、IM、游戏、网络媒体等丰富多彩的应用为主。

今天，网络已经成为社会生活的一个重要组成部分。在此过程中，出现了P2P、VoIP等业务，这些应用给客户带来丰富的互联网体验的同时，也给网络的运营者、管理者带来了巨大的影响，同时也不可避免地给网络的监管和网络技术提供者、设备制造商提出了新的挑战。

新应用对运营商的挑战

- 运营商的苦恼
  - 网络宽带设备的不断升级，依然无法跟上网络应用“多样化”带来的带宽需求；
  - 针对不同类型的流量如何进行分类计费策略？

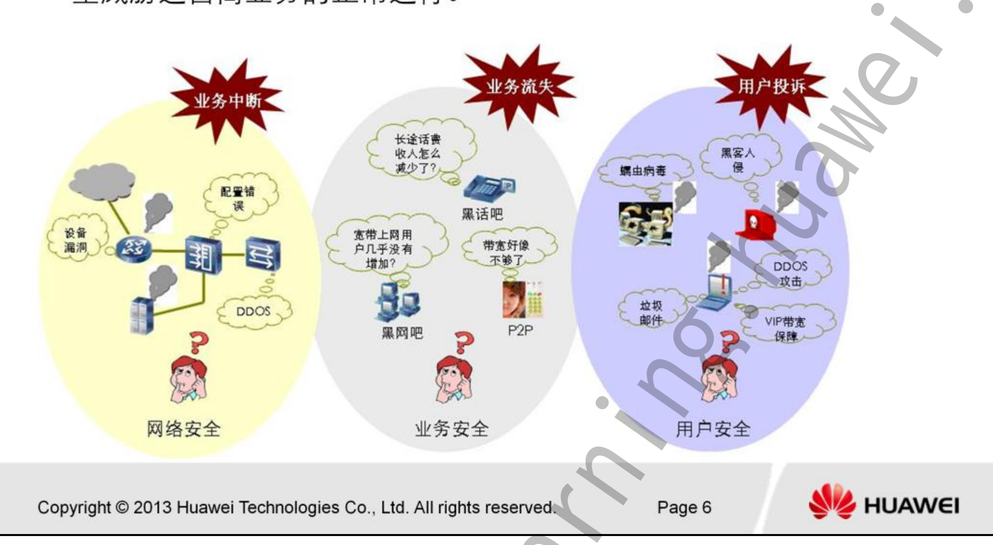




P2P、VoIP、共享接入等已经给网络运营带来极大的影响!



以2004年11月TOM－Skype在中国市场的推出为标志，高质量的网络电话开始盛行，其致命的杀手锏——免费性已经对传统电信运营商的语音业务造成了巨大的冲击。“电脑－电话”（PC to Phone）和“电话－电话”（Phone to Phone）等网络电话服务一旦实现，将彻底颠覆传统电话业务的市场格局，面对网络电话咄咄逼人的发展态势，传统电信运营商必须要适应和改变。



无监管的VoIP业务、无限制的P2P业务以及不受控的宽带私接对当前运营商带来的不仅是基本电信业务收入、带宽利用等威胁，同时随着高强度加密技术、P2P 技术和IM 技术的结合，给最终用户、企业网络和电信网络带来多方位的安全威胁(DDoS等网络攻击、蠕虫病毒以及SPAM等)，进一步提高了安全管理的技术难度和成本。伴随着电信业务IP化和互联网业务多媒体化的发展，电信网络正逐步走向基于IP承载网络的网络融合、业务融合和应用融合。

- 从不同应用角色看，政府、运营商、企业以及家庭 用户对网络的业务控制能力提出了各自的要求：
  - 从监管者角度来说，要求网络具备不良信息的识别和控制的能力，尤其是对反动、色情、赌博、暴力等不良信息的过滤；
  - 从运营商角度来说，要求网络能够对各类业务流量提供差异化的服务能力，尤其是保障电信级业务的服务质量，如软交换电话、3G语音以及大客户业务等；
  - 从企业角度来说，要求网络具备识别特定业务信息，并按照企业利益对信息进行处理的能力，整合复杂的IT防范设备，使得企业专注于核心业务；
  - 从家庭用户来说，结合健康上网的需求，要求网络具备个性化业务控制功能，尤其是对不良网站的屏蔽和网络游戏沉湎的防止。IP业务识别与控制的研究目的就是参考现有各标准化组织的研究成果，融合现有的各种产品和解决方案，提出通用的业务识别与控制架构。

新应用对企业网的挑战

- 企业管理的困惑
  - 公司业务的开展无法得到足够的带宽保障；
  - 员工在工作时间内的在线视频、聊天等行为，降低企业工作效率，并带来安全上的隐患。

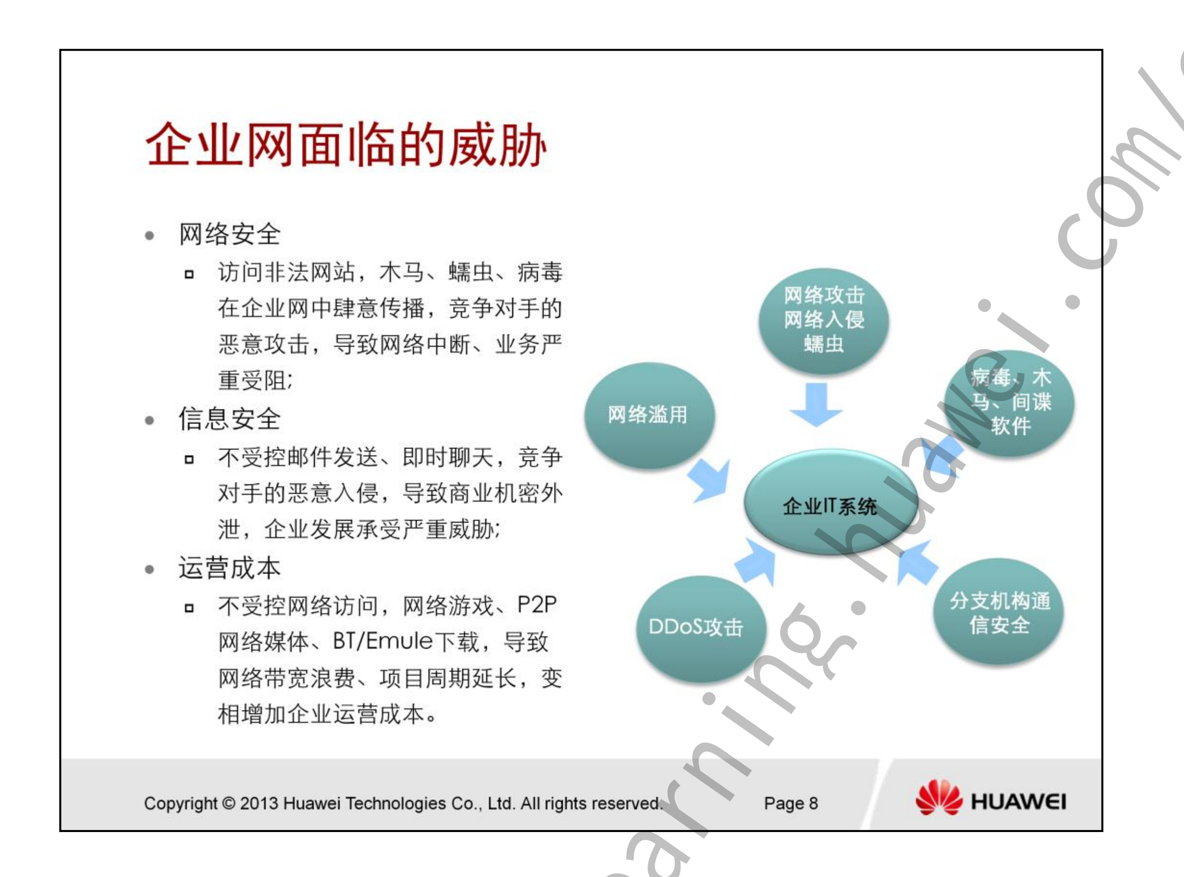




P2P、不可控的上网行为等已经给企业网络带来极大的影响!



不能对企业内部网络流量识别就不能这些流量进行有效控制，也就不能对公司员工行为进行监控。



互联网已经成为人类社会发展的一块基石，企业越来越依赖于互联网，企业在使用互联网的同时也承担着一定的风险：

- 企业及分支机构间的通信存在安全隐患，机密信息可能被恶意截获；
- DDoS、黑客入侵、木马、蠕虫、病毒等攻击手段的严重威胁企业业务运营；
- P2P下载、IM通信、浏览不良网站等网络滥用给企业带来了法律风险和安全隐患，影响了运营效率。



目录



传统业务识别技术

- 早期网络的业务流量分析，主要从物理端口、IP层和TCP/UDP层了解流量的状态。
- 端口检测根据TCP/UDP的端口来识别应用，检测效率高。但随着IP网络技术的发展，端口检测技术适用的范围越来越小。

DNS协议采用53端口；
BGP协议采用179端口；
RPC远程过程调用采用135号端口；
……





传统业务流量识别可以从流量物理接口，以及IP、TCP等包头信息进行流量识别，从而对特定数据流进行控制，但是对于新出现的业务流量则不能有效识别，进而不能有效控制这些流量。

传统方法无法满足现网流量分析

五元组

- 基于物理端口、IP层和TCP/UDP层了解流量状态
- 基于TCP/UDP的端口识别应用协议
- 基于IP的流量统计

端口误用与重用

数据流

- 以五元组的形式提供数据流的信息，用于分析用户的行为
- 典型：Netflow、NetStream等技术

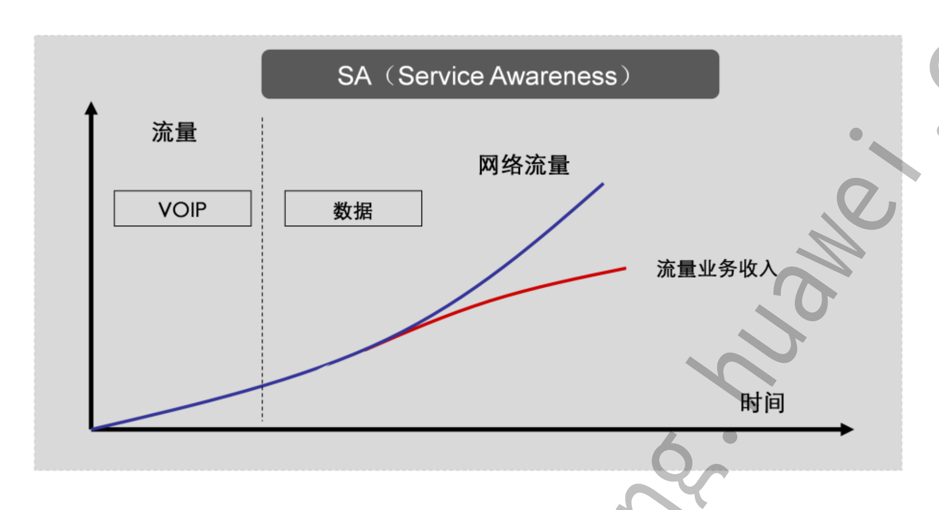
无法分辨业务类型

传统方法无法准确识别出网络流量中的应用协议类型



- 传统分析方法的不足：
  - 基于端口的检测一般效率较高，但无法处理端口误用及重用的情况，易产生误报和漏报，有相当大的局限性；
  - 基于流的分析和处理，已经比最初简单基于IP的流量统计更进了一步，朝着关注用户或用户群行为的方向发展，但还不能分辨出这些流量中的各种业务。

SA（Service Awareness）技术



- 准确感知流量中的应用，是保证网络可用性、可测量性和可管理性的必备技术手段！



SA（Service Awareness）提供对TCP/UDP传输层以上具体应用协议的识别功能，基于该功能，USG支持对网络流量按协议进行细分统计，对某些具体协议流量进行流量阻断或放行。

应用控制的5个重要应用领域：

- 网络智能化管理；
- P2P有效控制；
- QoS服务质量优化；
- 保证网络安全；
- 分层服务、管理及计费。



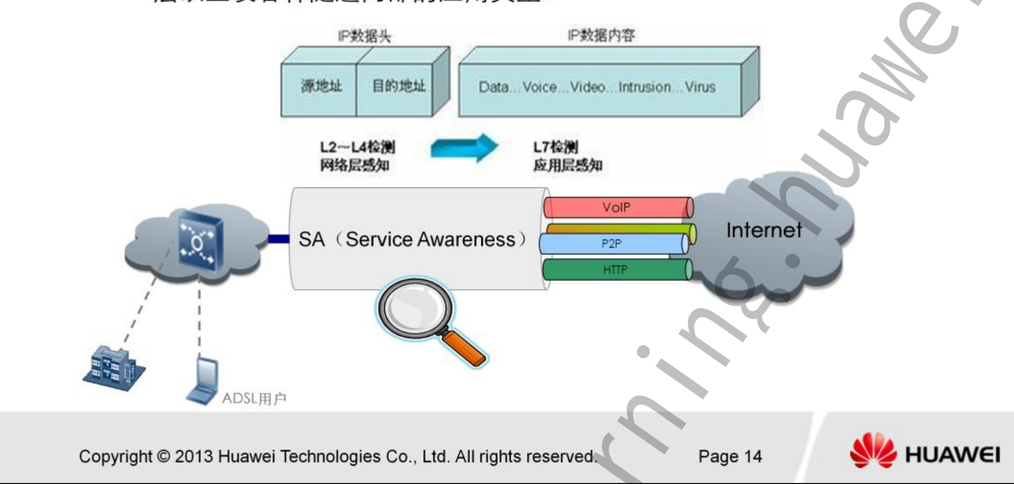
目录

1. 应用控制技术产生背景
2. **应用控制技术介绍**
   - 2.1 传统业务识别技术介绍
   - **2.2 SA识别技术介绍**
3. 应用控制技术应用



业务感知技术介绍

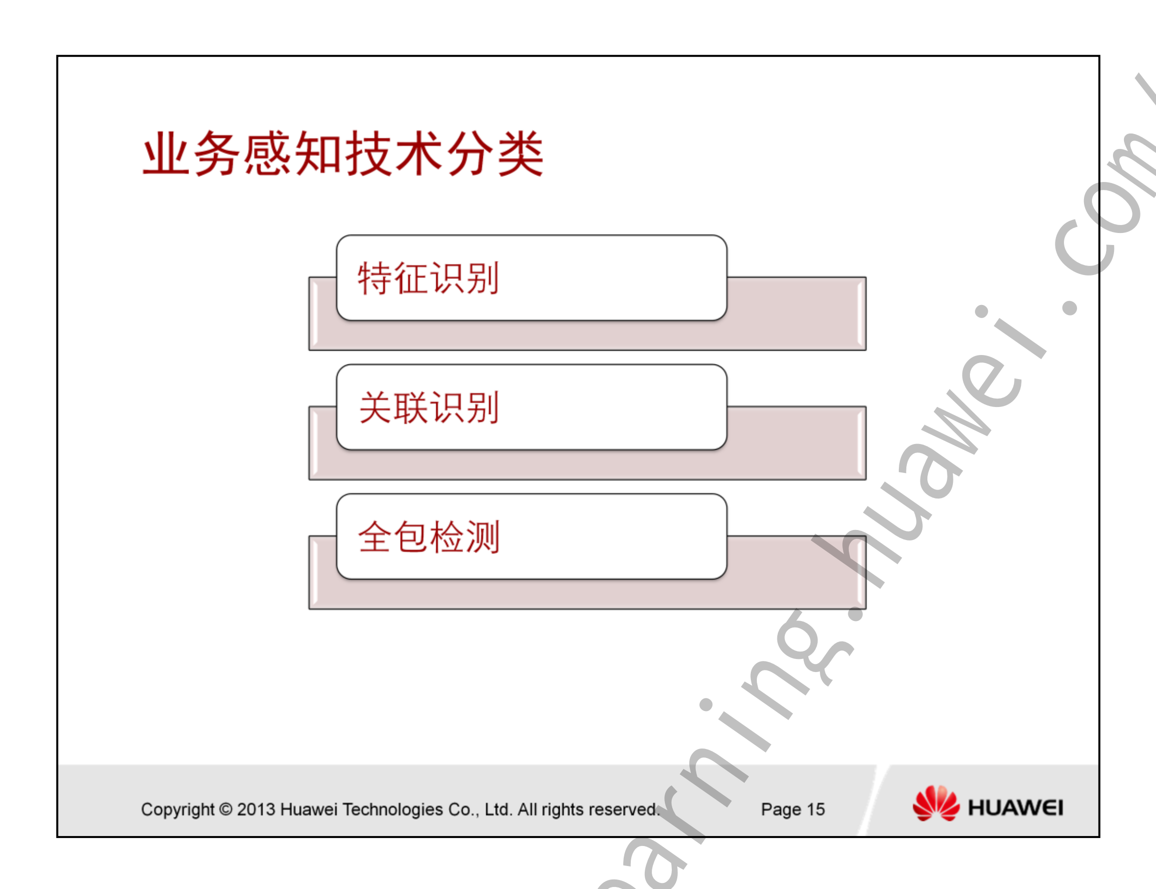
- 定义
  - 通过对报文的应用层数据进行内容检测，分析报文或流在IP和UDP/TCP层以上及各种隧道内部的应用类型。



应用控制是一种通过SA技术对网络中的报文进行识别控制的应用功能。SA即业务感知，通过对报文的应用层数据进行内容检测，分析报文或数据流在IP和TCP/UDP层以上的应用业务类型，从而进行流量识别和流量管理以及其他增值服务。

SA的价值:

- 流量识别；
- 流量管理；
- 内容计费；
- 内容安全。



很多情况下，对业务的识别是综合运用多种技术，才能达到很好的效果。SA主要有特征检测、关联识别和全包检测。

- 特征识别：新兴的P2P应用、VoIP应用，在一个常用端口范围之外，也可以随机选取任意端口进行通信。因此，要识别这些协议，无法单纯依赖端口检测，而必须在应用层对这些协议的特征进行识别，应用层特征识别，大致分为两种：
    - 一种是已知协议的识别，例如FTP、HTTP、DNS、SMTP等，有标准的协议，并规定了特有的消息和命令字以及状态迁移机制，通过分析应用层内的这些专有字段和状态，就可以精确可靠地识别这些协议。
    - 另一种是未公开协议的识别，例如当前多数的P2P协议、IM、VoIP协议。出于多方面的考虑，并不公开其协议细节，这时一般需要通过逆向工程分析协议机制，通过报文流的特征字段来识别该通信流量。这类方法工作量大，而且协议的变化快，要保持各种协议变化的及时跟踪，必须有大量的人力投入和不断的技术跟踪才能保证检测的高效性，因此要有较强大的研发队伍作后盾。
- 关联识别：某些数据流，控制通道和数据通道是分开的（如FTP、SIP、H.323等），一般的处理方式是对这些会话分别进行识别，这可能导致分析速度较慢或影响对数据通道的识别。关联协议识别，是将来自同一源地址的控制通道和后续的数据通道进行关联的技术，从而达到快速识别的目的。
- 全包检测：某些协议的报文是承载在其他协议上进行传输的，如MSN信息可能通过HTTP协议承载、VoIP信息可能通过IM类型协议承载。全包检测即对这种类型的报文的所有字节进行检测，以提高对协议的识别准确率。USG支持对指定的协议启用全包检测功能。

SA业务识别技术

- 加密协议识别能力
  - 能够准确的识别出BT加密、Vagaa加密、PPLive加密、迅雷加密、Skype等数十种加密应用，对常见的加密P2P应用和加密VOIP应用可以准确的识别和阻断。
- 业务细分能力
  - 随着越来越多的软件将多种业务融合到一起，对同一应用软件下的多种业务进行区分和控制。
- 准确高效的行为识别能力
  - 高效的行为识别模型，能够在应用的模式特征发生变化之后依然进行准确的识别，该模型在识别和控制新出现的、未知的P2P应用方面效果显著。



- 加密协议识别能力：众所周知，当前许多应用为了逃避检查和控制，都对传输的数据进行了加密，SA在检测加密应用方面，经过多年的技术积累，总结出了一套特征、行为加统计的综合检测模型，能够准确的识别出BT加密、Vagaa加密、PPLive加密、迅雷加密、Skype等数十种加密应用，对常见的加密P2P应用和加密VOIP应用可以准确的识别和阻断。
- 业务细分能力：随着越来越多的软件将多种业务融合到一起，对同一应用软件下的多种业务进行细分并分别控制就显得越来越有必要了，例如，QQ融合了文字聊天、文件传输、语音、视频、游戏等多种业务功能。我们的SA在软件业务细分方面走在了行业的前列，几乎所有的应用软件，都可以按照其业务类型的不同，分别进行区分和控制。
- 准确高效的行为识别能力：为了应对层出不穷的新应用，以及现有软件的频繁升级，SA采用了一套高效的行为识别模型，并已获得多项专利，该行为识别模型有很好的性能和准确性，另外还有很好的适应性，能够在应用的模式特征发生变化之后依然进行准确的识别，该模型在识别和控制新出现的、未知的P2P应用方面效果显著。

SA业务流程

- 流量解析引擎负责加载协议特征知识库，对输入的7层数据进行识别，输出识别出的各类协议或应用的类型。

知识库升级服务
知识库升级系统
知识库管理
待处理数据流
网络数据流预处理
流量解析引擎
基于协议类型的网络数据流/网络报文处理

某些数据流，控制通道和数据通道是分开的（如FTP、SIP、H.323等），一般的处理方式是对这些会话分别进行识别，这可能导致分析速度较慢或影响对数据通道的识别。关联协议识别，是将来自同一源地址的控制通道和后续的数据通道进行关联的技术，从而达到快速识别的目的

关联协议识别可以将同一应用协议的控制通道流和数据通道流关联起来。通过对控制通道流的分析，可以分析出通讯双方将要在哪个通道上建立何种类型的数据流，并在协议识别时将控制通道流和该控制通道流协商出来的数据通道流关联起来。USG在对控制通道流进行深度解析时，提取出其中协商的数据通道流的源三元组和目的三元组信息，并加入关联表。在后续识别过程中，可以通过该关联表项对数据通道流快速识别。

一般情况下，USG对报文的特定字节进行协议特征检测，对于多数已知协议可以做到成功检测。某些协议的报文是承载在其他协议上进行传输的，如MSN信息可能通过HTTP协议承载、VoIP信息可能通过IM类型协议承载。全包检测即对这种类型的报文的所有字节进行检测，以提高对协议的识别准确率。USG支持对指定的协议启用全包检测功能。

流量解析引擎

特征识别

- 通过模式匹配算法，根据已知协议的内容特征，对网络报文的应用层内容进行匹配检索
- 单包匹配、多包匹配、多流匹配

关联识别

- 对通讯控制通道和数据传输通道分开的应用协议，将多个通道流量进行协同检测
- 对于某些业务类型已经判定的流量，可以通过三元组对与同一主机端口进行通讯的不同流量进行关联判断

全包检测

- MSN信息可能通过HTTP协议承载、VoIP信息可能通过IM类型协议承载。全包检测即对这种类型的报文的所有字节进行检测，进行识别处理





目录

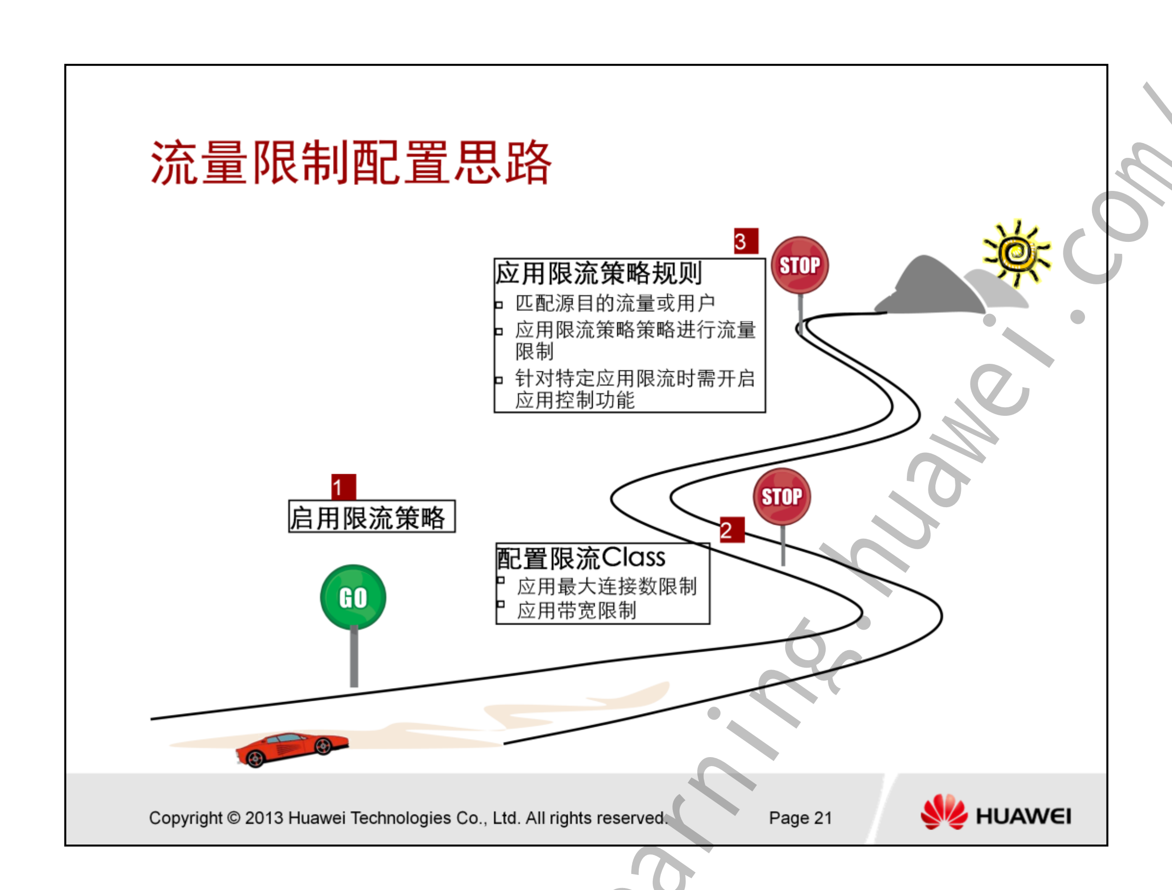


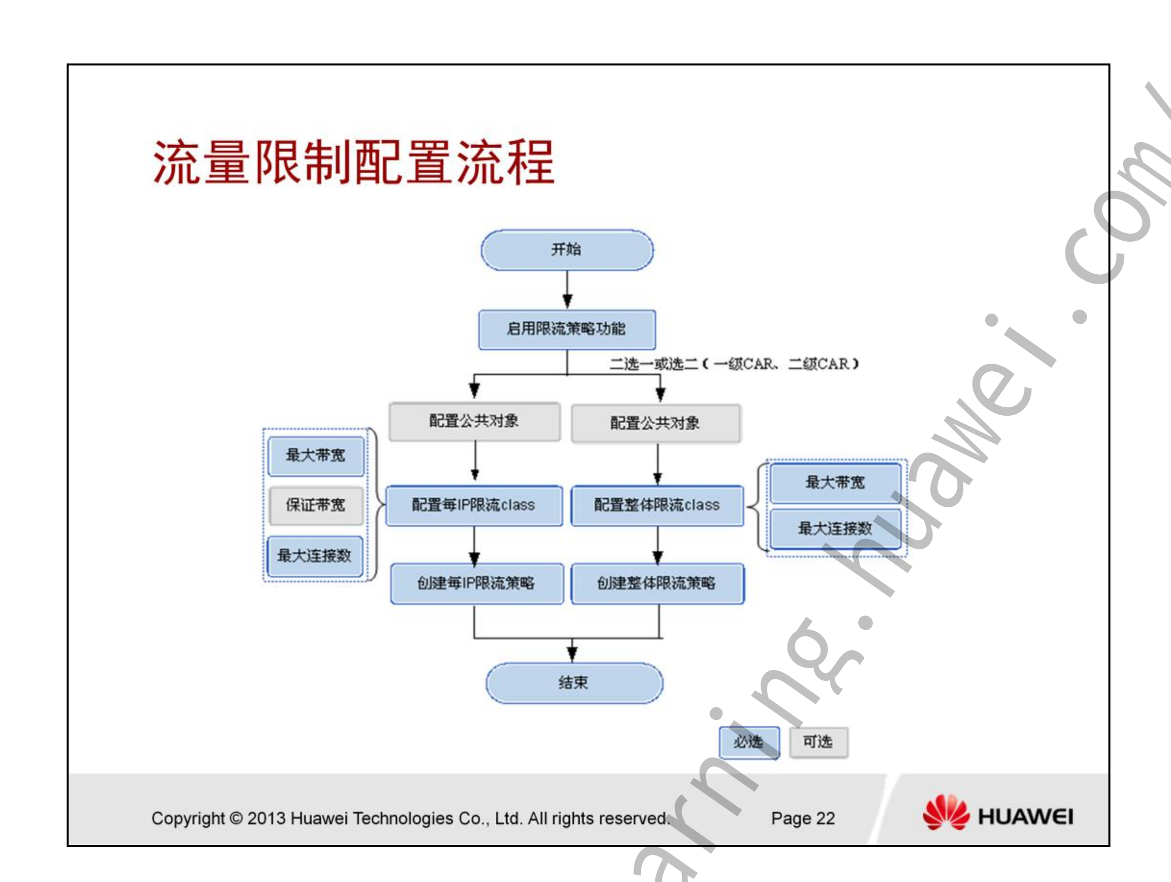
应用场景

- **流量限制**
  - 连接数限制：对指定用户，IP地址或者网络发起的连接数量或接收的连接数量进行限制。
  - 带宽限制：对指定用户，IP地址或者网络的带宽进行限制。
- **流量阻断**
  - 是对数据流中的应用层数据进行内容检测的技术。在匹配成功后，根据应用的需求，可以对识别的网络流量进行允许通过、阻断的控制动作。



可以通过应用控制检测识别特定应用数据流，然后使用流量限制对这些应用数据流进行限速和限连接数。


流量限制配置思路
3
应用限流策略规则
匹配源目的流量或用户
应用限流策略策略进行流量限制
针对特定应用限流时需开启应用控制功能
STOP
1
启用限流策略
GO
2
配置限流Class
应用最大连接数限制
应用带宽限制
STOP
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 21
HUAWEI


流量限制配置流程
开始
启用限流策略功能
二选一或选二（一级CAR、二级CAR）
配置公共对象
配置公共对象
最大带宽
保证带宽
最大连接数
配置每IP限流class
配置整体限流class
最大带宽
最大连接数
创建每IP限流策略
创建整体限流策略
结束
必选
可选
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 22
HUAWEI



- 命令行配置：

  执行命令system-view，进入系统视图。

  执行命令traffic-policy enable，启用限流策略功能。

配置限流Class

防火墙 > 限流策略 > 每IP限流

每IP限流 | 每IP限流Class

新建每IP限流Class

名称	Download限制	*
保证带宽	50	<8-10000000>kbps
最大带宽	100	<8-10000000>kbps
最大连接数	10000	<1-1000000>

应用 返回

防火墙 > 限流策略 > 整体限流

整体限流 | 整体限流Class

新建整体限流Class

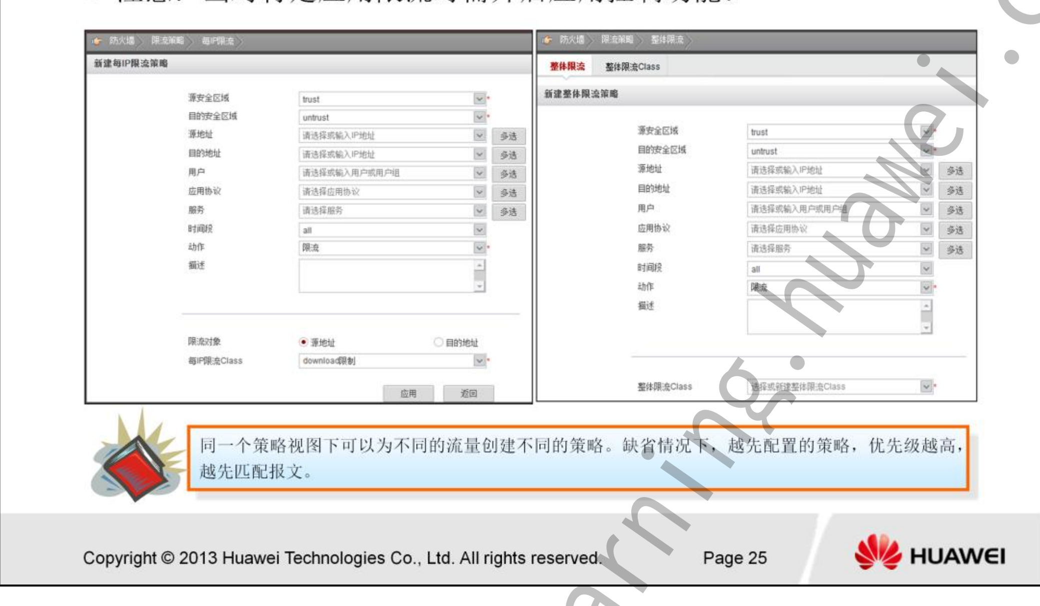
名称		*
最大带宽		<8-10000000>kbps
最大连接数		<1-1000000>

应用 返回

保证带宽需要与整体限流结合起来使用，因为对于单个IP而言，若不配置其所在网络的整体限流，单个IP的最大带宽就相当于保证带宽，此时配置保证带宽没有意义。

HUAWEI

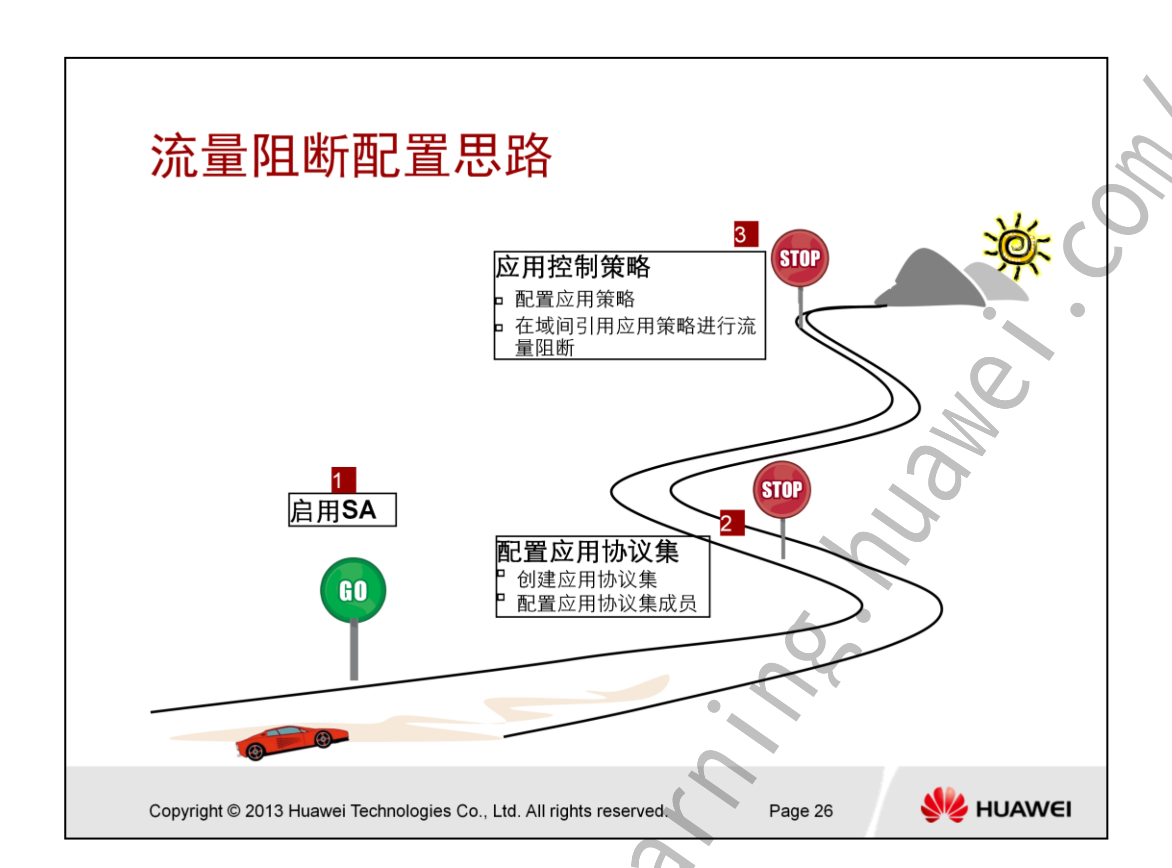
- 命令行配置：
  - 执行命令car-class car-class-name type per-ip [vpn-instance vpn-instance name]，进入每IP car-class视图。
  - 执行命令car-class car-class-name type shared [vpn-instance vpn-instance name]，进入整体car-class视图。
  - 执行命令car { max max-value | guaranteed guaranteed-value }，配置最大带宽和保证带宽，保证带宽不大于最大带宽。二者值范围都8～10000000，单位：kbps。
  - 执行命令connection-number connection-number，配置最大连接数。取值范围是1～1000000。



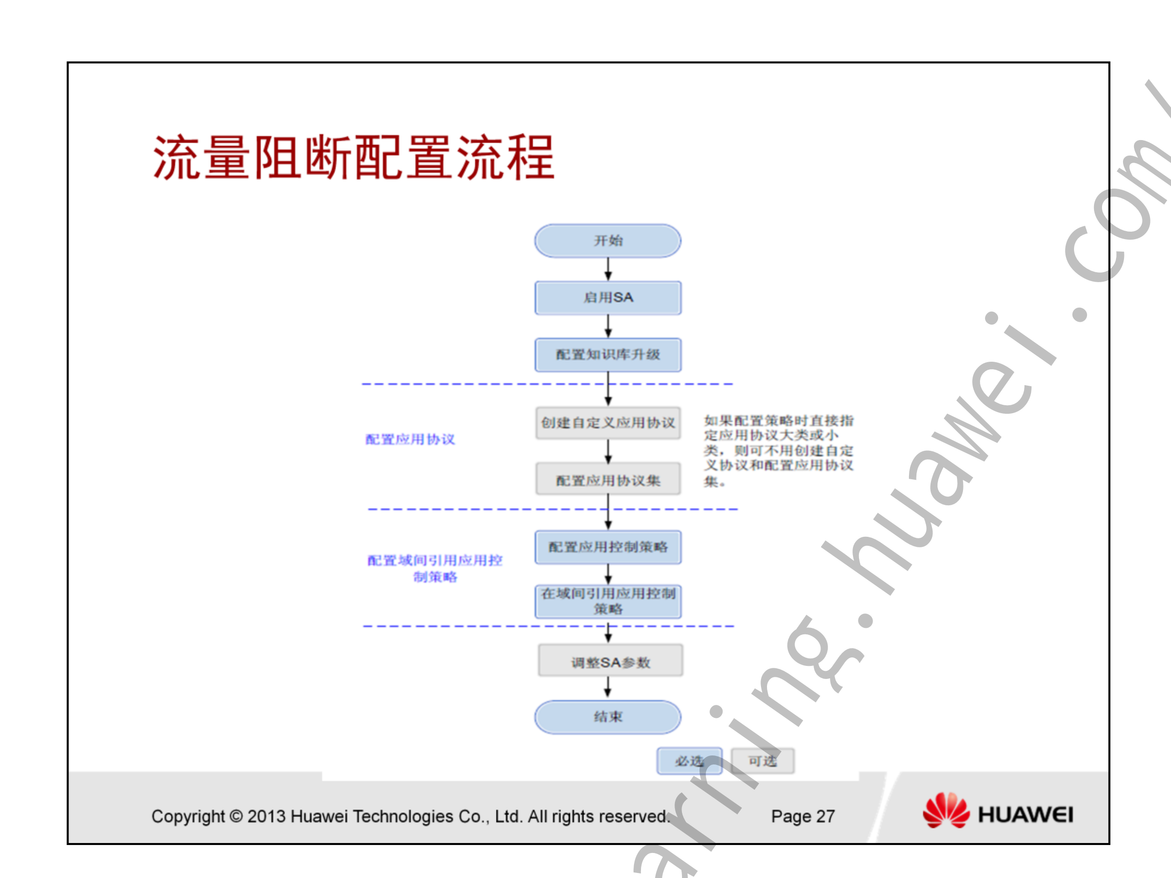
- 命令行配置：
  - 进入域间配置每IP限流策略视图：

  traffic-policy interzone [vpn-instance vpn-instance-name] zone-name1 zone-name2 { outbound | inbound } per-ip

  - 执行命令policy [policy-id]，进入该条策略的配置视图。 同一个策略视图下可以为不同的流量创建不同的策略。缺省情况下，越先配置的策略，优先级越高，越先匹配报文。
  - 执行命令policy car-type { source-ip | destination-ip }，选择针对源IP或者目的IP进行每IP限流。
  - 执行命令policy car-class car-class-name，配置每IP限流策略引用car-class，缺省情况下，针对源IP进行限流。


流量阻断配置思路
3
应用控制策略
配置应用策略
在域间引用应用策略进行流量阻断
STOP
1
启用SA
GO
2
配置应用协议集
创建应用协议集
配置应用协议集成员
STOP

HUAWEI


流量阻断配置流程
开始
启用SA
配置知识库升级
配置应用协议
创建自定义应用协议
配置应用协议集
如果配置策略时直接指定应用协议大类或小类，则可不用创建自定义协议和配置应用协议集。
配置域间引用应用控制策略
配置应用控制策略
在域间引用应用控制策略
调整SA参数
结束
必选
可选
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 27
HUAWEI



进入应用控制策略界面启用应用控制功能：



HUAWEI

- 命令行配置：

  执行命令system-view，进入系统视图

  执行命令sa enable，启用SA功能

知识库升级

- 本地升级步骤：
  - 执行命令system-view，进入系统视图
  - 执行命令**update rule-base file** *filename*，进行知识库本地升级。
  - Info: Current Version is **0.0.0.0**,the New Version is **2.0.0.132**,Continue[Y/N]:
  - 确认当前版本和新版本知识库后，输入**Y**并按下“Enter”键确认，进行升级。
- 设备提示如下信息，则表示升级成功：

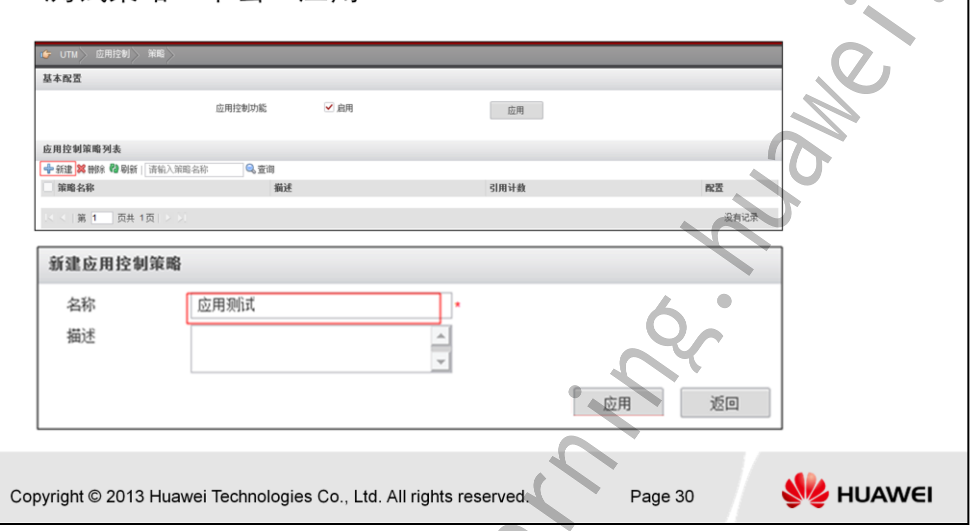
Info: Succeeded in updating SA to version **2.0.0.132**.



自动和手动远端升级请查看相关产品文档，注意升级知识库对设备内存的要求是不得少于8M。

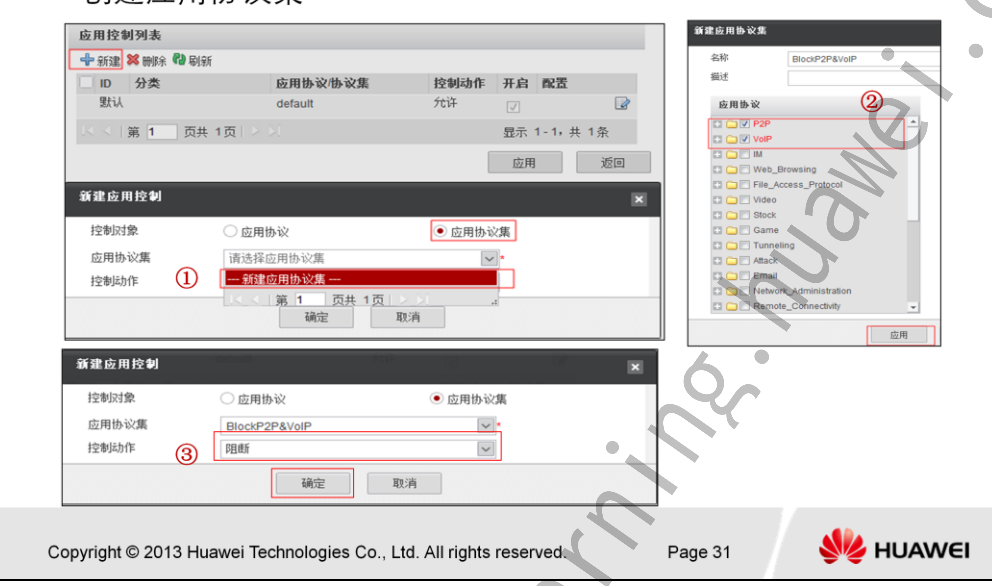
创建应用控制策略

- 创建应用控制策略：在应用策略界面点击“增加”创建“应用测试策略”单击“应用”。



配置应用协议集

- 创建应用协议集

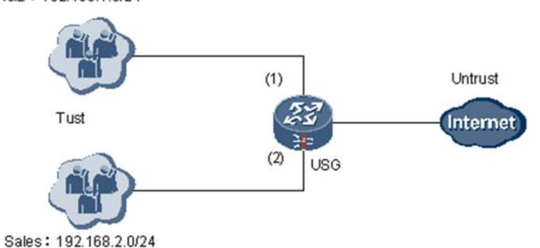


- 命令行配置说明：
  - 执行命令system-view 进入系统视图。
  - 执行命令sa-policy *policy-name* [vpn-instance vpn-instance name]，进入sa策略视图。
  - 执行命令policy default action { permit | deny }，配置策略的默认动作。
  - 当数据流不能匹配该策略的任一规则时，将执行该默认动作。缺省配置是permit。
  - 执行命令rule [rule-id]，创建并进入SA策略规则视图。
  - 执行命令rule { app-set app-set-name | category category-name [application application-name] | category userdefine application application-name }，配置SA策略的规则引用的应用协议类型。
  - 执行命令action { permit | deny }，配置策略规则的动作。缺省为permit。
  - 执行命令rule enable 启用策略。



- 命令行配置说明：
  - 进入域间安全策略视图：policy interzone [vpn-instance vpn-instance-name] zone-name1 zone-name2 { inbound | outbound }
  - 执行命令policy [policy-id]，创建转发策略，并进入策略ID视图。
  - 执行命令action { permit | deny }，配置域间安全策略的动作。
  - 执行命令policy sa sa-policy-name，应用策略。

流量阻断配置举例

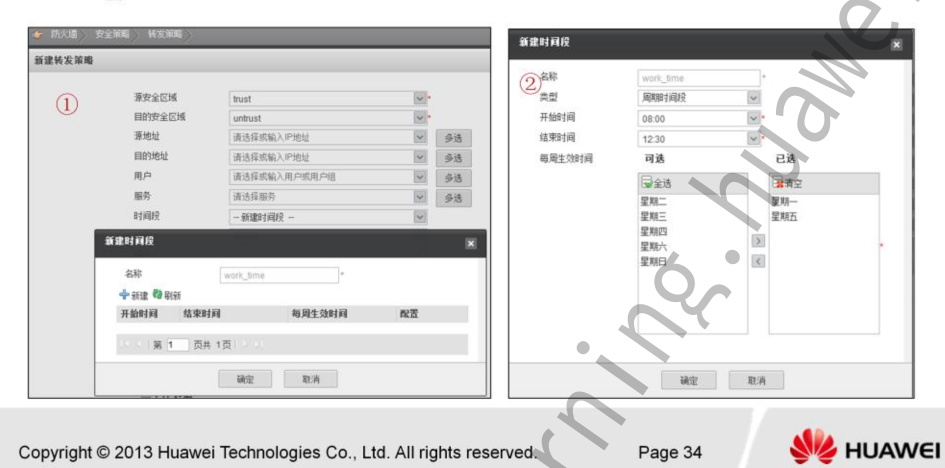


- 组网需求
  - 某公司通过内网研发和销售人员分别分配在192.168.1.0/24网段和192.168.2.0/24网段，有如下业务需求：
  - 内网研发部门人员在工作时间周一至周五的8:00～12：30，14：00-18:00不能使用IM（Instant Messaging）功能。
  - 内网销售部门人员在所有工作时间可以正常使用IM功能。



流量阻断配置（一）

- 配置USG，使内网用户可以访问因特网。（略）
- 配置时间范围，设定为周一至周五的8:00-12：30，14：00-18:00，命名为work_time。。



配置USG，使内网用户可以访问因特网。（略）

配置时间范围，设定为周一至周五的8:00-12：30，14：00-18:00，命名为work_time

[USG] time-range work_time 8:00 to 12:30 working-day [USG] time-range work_time 14:00 to 18:00 working-day



启用SA功能，并配置策略im_block，对IM类型的协议进行检测，并对检测到的IM协议执行阻断动作。

[USG] sa enable

[USG] sa-policy im_block

[USG-sa-policy-im_block] policy default action permit （当没有匹配rule缺省的动作)

[USG-sa-policy-im_block] rule 1

[USG-sa-policy-im_block-1] rule category IM

[USG-sa-policy-im_block-1] action deny

[USG-sa-policy-im_block-1] quit

[USG-sa-policy-im_block] quit

流量阻断配置（三）

- 配置转发策略，在域间应用SA策略im_block，实现对192.168.1.0/24网段的研发人员在work_time时间段内的IM即时通讯的阻断。





HUAWEI

配置Trust和Untrus的域间包过滤，使192.168.2.0/24网段的销售人员能正常通讯。在域间应用SA策略im_block，实现对192.168.1.0/24网段的研发人员在work_time时间段内的IM即时通讯的阻断。

```
[USG] policy interzone trust untrust outbound
[USG-policy-interzone-trust-untrust-outbound] policy 0
[USG-policy-interzone-trust-untrust-outbound-0] policy source 192.168.2.0 mask 24
[USG-policy-interzone-trust-untrust-outbound-0] action permit
[USG-policy-interzone-trust-untrust-outbound] policy 1
[USG-policy-interzone-trust-untrust-outbound-1] policy source 192.168.1.0 mask 24
[USG-policy-interzone-trust-untrust-outbound-1] policy time-range work_time
[USG-policy-interzone-trust-untrust-outbound-1] action permit
[USG-policy-interzone-trust-untrust-outbound-1] policy sa im_block
[USG-policy-interzone-trust-untrust-outbound] policy 2
[USG-policy-interzone-trust-untrust-outbound-2] policy source 192.168.1.0 mask 24
[USG-policy-interzone-trust-untrust-outbound-2] action permit
```

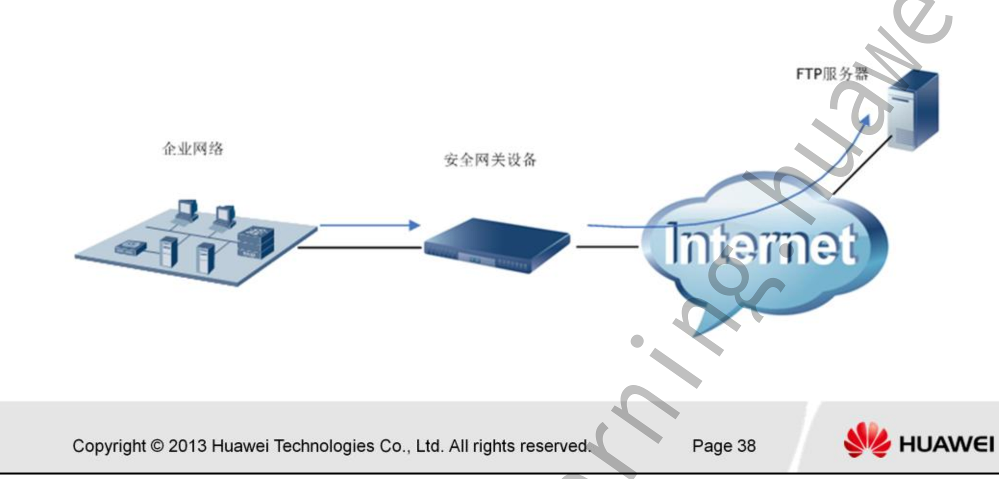


目录

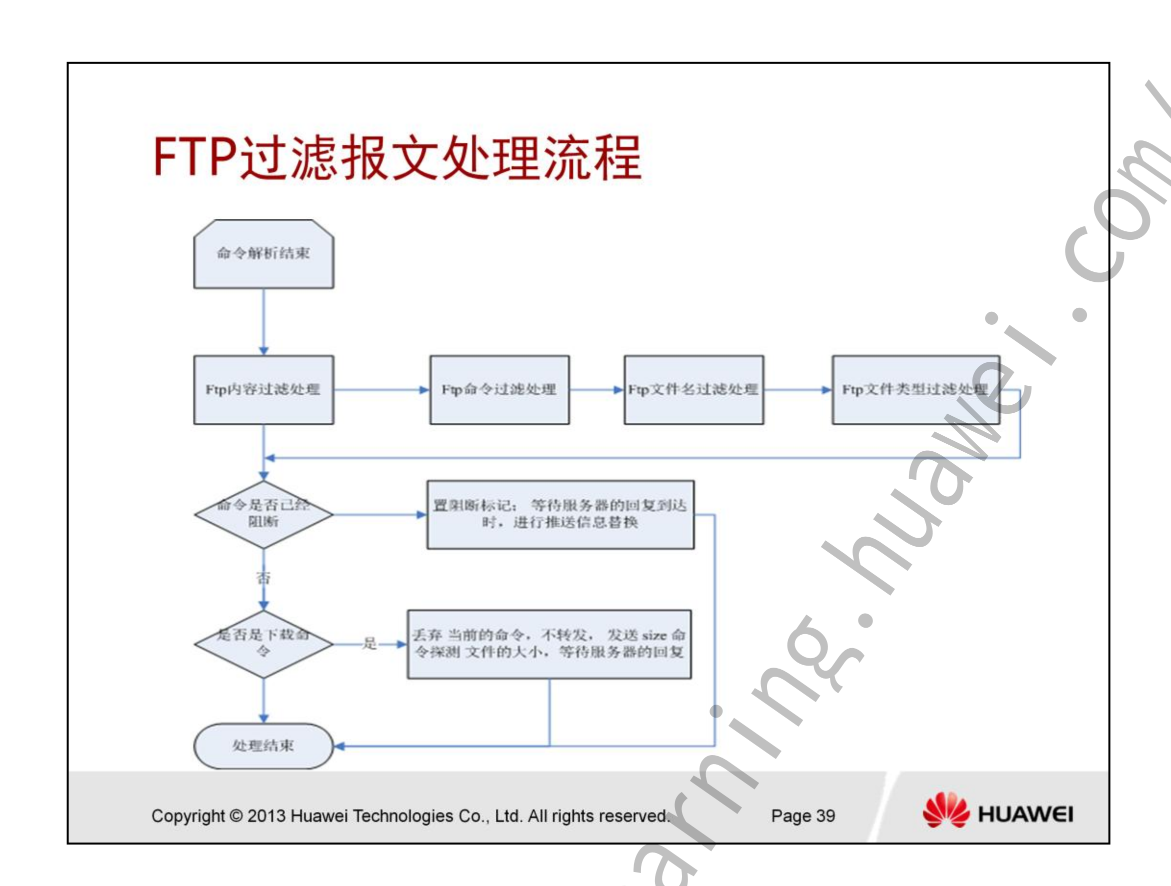




- FTP过滤概述：理解用户传输的信息类型，过滤无关信息的获取，阻止企业内部数据的外传企图。
- 启用该功能的设备，通常应用于企业与互联网的网络边界。

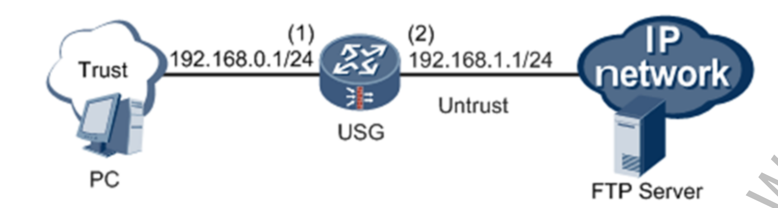


FTP主要功能是向用户提供本地和远程主机之间的文件传输。在进行版本升级、日志下载、文件传输和配置保存等业务操作时，FTP功能被广泛地使用。如果FTP操作不受控，会给网络带来较多不可控的威胁。通过FTP过滤，可以对FTP操作（上传、下载、删除）、上传/下载的文件名、文件类型、文件大小进行控制。



注意：FTP过滤功能受License控制。

FTP过滤配置举例



- 组网需求
  - 如图1所示，公司部署FTP服务器，为员工提供FTP服务。为规范员工对FTP的操作，公司制定以下策略：
    - 禁止FTP delete操作。
    - 禁止下载文件名包含dota或craft的文件。
    - 禁止下载文件类型为mp3、wmf的文件。
    - 禁止上传和下载超过10000KByte的文件。



FTP过滤配置（一）

- 配置USG，使内网用户可以访问因特网。（略）
- 配置为UTM模式并启动FTP过滤功能。

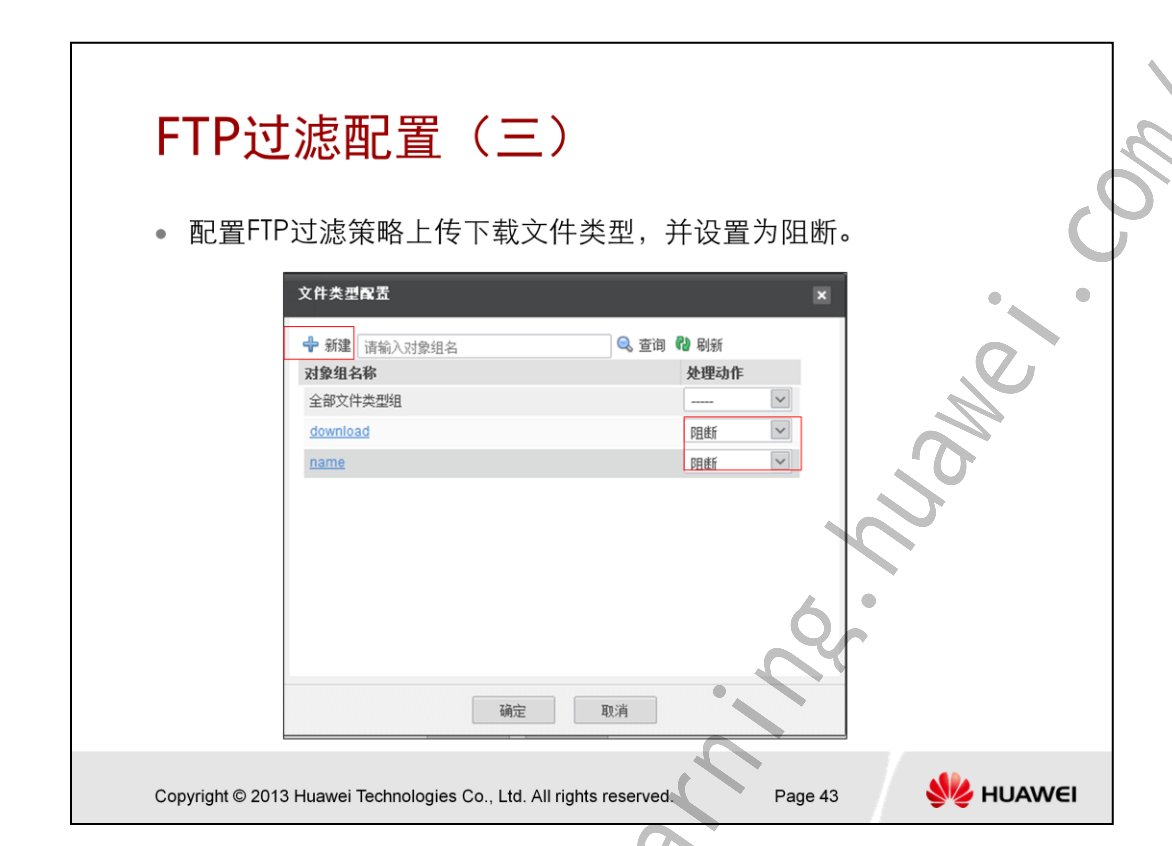


- [USG] runmode utm
- [USG] ftp-filter enable

FTP过滤需要License支持，否则FTP过滤不生效。



通过FTP过滤，可以对FTP操作（上传、下载、删除）、上传/下载的文件名、文件类型、文件大小进行控制。



- Device上开启FTP过滤功能后，当用户进行FTP的upload、download或delete操作时，Device会对FTP操作进行解析：
  - 如果用户的FTP操作匹配FTP过滤策略，执行过滤策略（阻断或告警）。
  - 如果用户的FTP操作没有匹配FTP过滤策略，则允许该FTP操作。

FTP过滤配置（四）

- 配置转发策略，在域间应用FTP过滤策略FTP。

防火墙 > 安全策略 > 转发策略

源安全区域	trust	
目的安全区域	untrust	
源地址	请选择或输入IP地址	多选
目的地址	请选择或输入IP地址	多选
用户	请选择或输入用户或用户组	多选
服务	请选择服务	多选
时间段	all	
动作	permit	
描述		

- [ ] IPS
- [ ] AV
- [ ] Web过滤
- [ ] 邮件过滤
- [x] FTP过滤

FTP过滤策略：ftp

- [ ] 应用控制
- [ ] 记录日志
- [ ] 开启策略会话流量统计

应用　返回

HUAWEI



总结

- 应用控制的产生的背景
- 应用控制的主要技术手段
- 应用控制技术的应用及配置



思考题

- 单选题
  1. 下列描述属于特征检测特点的是?

  A、对通讯控制通道和数据传输通道分开的应用协议，将多个通道流量进行协同检测。

  B、对于某些业务类型已经判定的流量，可以通过三元组对与同一主机端口进行通讯的不同流量进行关联判断。

  C、通过模式匹配算法，根据已知协议的内容特征，对网络报文的应用层内容进行匹配检索。

  D、通过分析各种应用的连接数、单IP的连接模式、上下行流量的比例、数据包发送频率等指标来区分应用类型。

- 判断题
  1. 关联识别技术用来对多通道的应用进行关联识别和分析。



习题与答案:

1、下列描述属于特征检测特点的是?

A、对通讯控制通道和数据传输通道分开的应用协议，将多个通道流量进行协同检测

B、对于某些业务类型已经判定的流量，可以通过三元组对与同一主机端口进行通讯的不同流量进行关联判断。

C、通过模式匹配算法，根据已知协议的内容特征，对网络报文的应用层内容进行匹配检索。

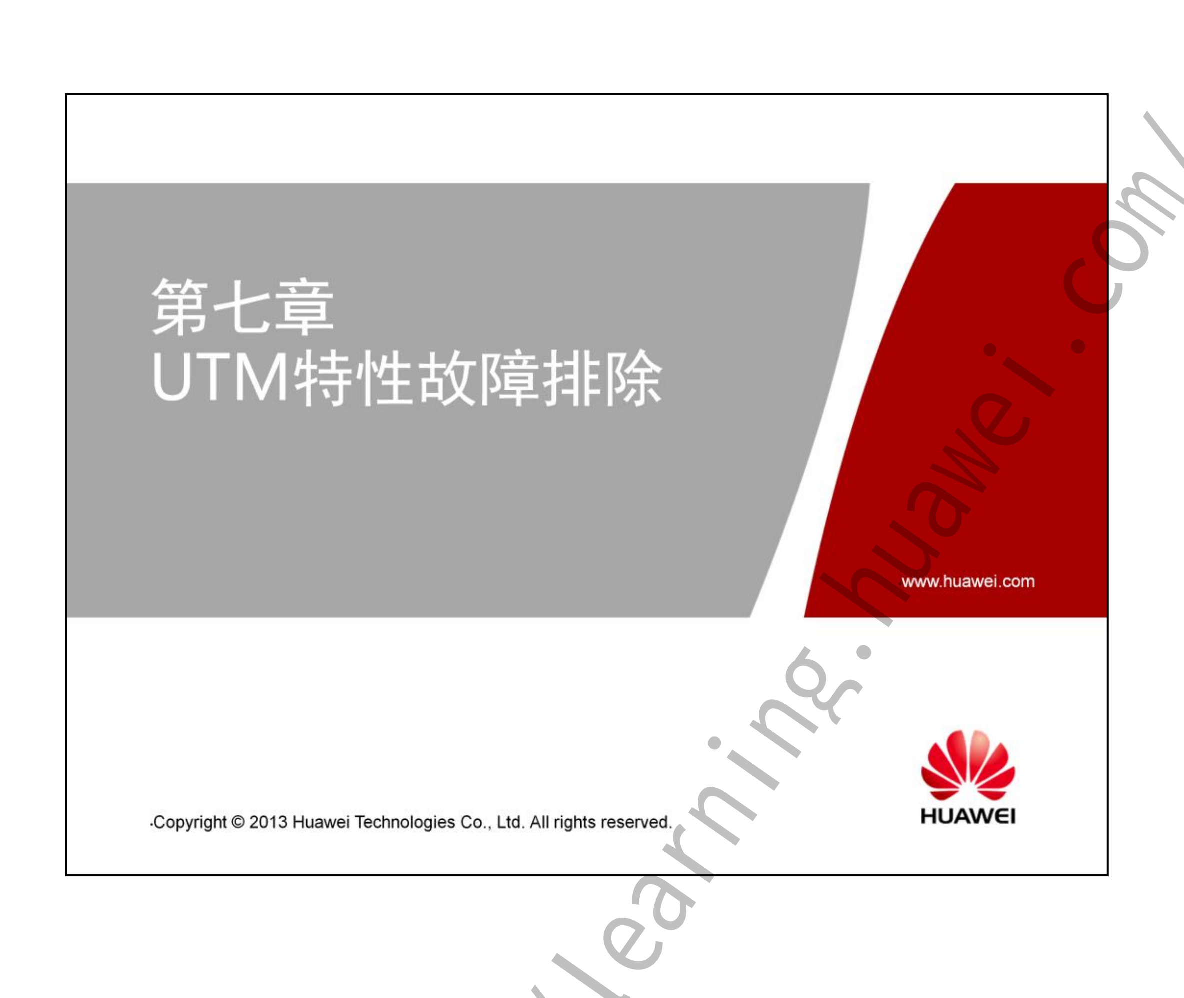
D、通过分析各种应用的连接数、单IP的连接模式、上下行流量的比例、数据包发送频率等指标来区分应用类型。

答案：C

2、 关联识别技术用来对多通道的应用进行关联识别和分析。

答案：正确


Thank you
www.huawei.com


第七章
UTM特性故障排除
www.huawei.com
HUAWEI



目标

- 学完本课程后，您将能够:
  - 掌握UTM故障排除
  - 掌握IPS常见故障排除；
  - 掌握AV常见故障排除;
  - 掌握URL过滤常见故障排除;
  - 掌握RBL过滤常见故障排除;
  - 掌握上网行为管理故障排除。





目录



UTM功能整体失效

- 现象描述：
  - 配置的UTM功能如IPS、AV、RBL过滤、URL过滤均失效。
- 可能原因：
  - 原因一：License不存在或过期。
  - 原因二：运行模式切换到了防火墙模式。
  - 原因三：禁用了防火墙状态检测机制。
  - 原因四：开启了二层快转功能。



排查步骤（1）

- 原因一：License不存在或过期。
  - 执行命令display license，查看License是否存在或过期。
    - 如果License不存在或过期，请购买并导入License。
    - 如果License未过期，继续执行原因二。
- 原因二：运行模式切换到了防火墙模式。
  - 执行命令display runmode，查看当前运行模式。
    - 如果运行模式为UTM，请执行原因三，继续进行故障排除。
    - 如果运行模式为Firewall，请在系统视图下执行命令**runmode utm**将运行模式切换到UTM。如果问题还没有解决，请执行原因三。



- 在USG防火墙执行：
  - <USG> display runmode

    Current runmode: UTM/Firewall

排查步骤（2）

- 原因三：禁用了防火墙状态检测机制。
  - 执行命令display current-configuration | include link-state，查看防火墙状态检测机制是否开启。
    - 如果防火墙状态检测机制已经开启，请继续执行原因四。
    - 如果防火墙状态检测机制为关闭，请开启。
- 在系统视图下执行firewall session link-state check，启用防火墙状态检测机制。
  - <USG> system-view
  - [USG] firewall session link-state check



- 检查是否开启防火墙状态检测：
  - <USG> display current-configuration | include link-state

    firewall ipv6 session link-state check

    undo firewall session link-state check tcp

    undo firewall session link-state check icmp

排查步骤（3）

- 原因四：开启了二层快转功能。
  - 执行命令display current-configuration | include l2fwdfast，查看二层快转功能是否开启。
    - 如果二层快转功能已经禁用，请联系技术支持。
    - 如果二层快转功能启用，请关闭。
- 在系统视图下执行命令undo l2fwdfast enable，禁用二层快转功能。
  - <USG> system-view
  - [USG] undo l2fwdfast enable



- 检查是否开启二层转发功能：
  - <USG> display current-configuration | include l2fwdfast

    l2fwdfast enable/disable
- 按照以上排查步骤执行后任然不能排除故障，请联系华为工程师。



目录

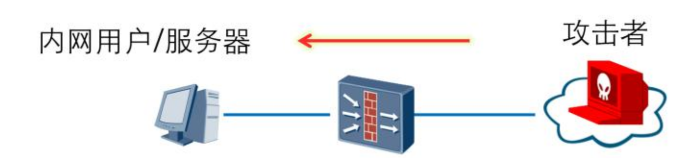


IPS配置注意事项

- 为了提高检测的精准度，请不要将分片重组功能关闭
- 当签名的协议配置为http时，只检测http头信息并不检测body内容
- 所有UTM特性都依赖于状态检测开关,该开关必须打开。
  - Firewall session link-state check，该命令开关在utm模式下应该是默认开启的，主要是检查是否存在用户误操作造成该开关被关闭。



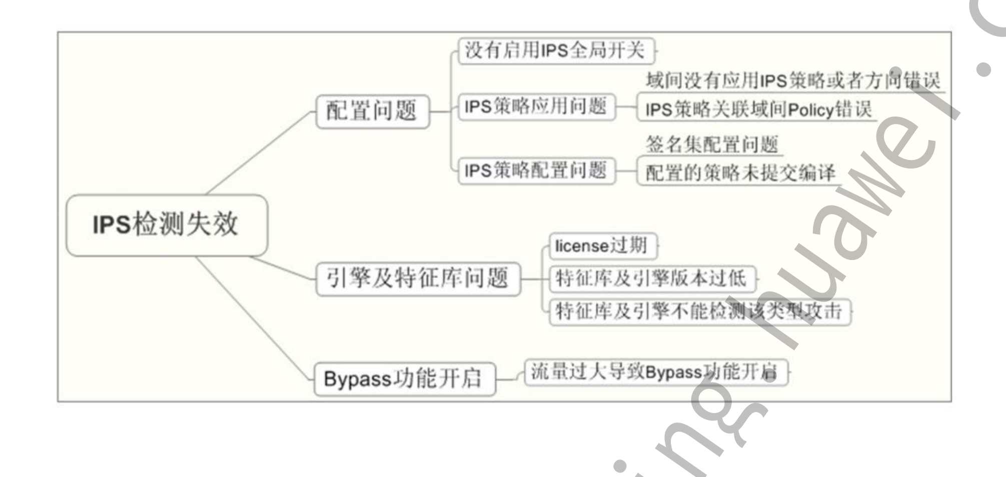
IPS检测失效故障排除



- 现象描述
  - 内网的用户或者服务器受到Internet的某类攻击，USG未产生IPS攻击告警，即IPS攻击检测失效。



IPS检测失效故障排除思路







- IPS global switch表示IPS全局开关的使能状态。如果状态为enable，表示使能。如果状态为disable，表示未开启。



- 域间方向判断依据为访问发起的方向，关联域间policy的时候需要注意policy的匹配顺序为顺序匹配，匹配到一条策略后不再往下匹配。

原因一：配置问题

- IPS策略配置问题
  - 执行命令display ips policy policy-name，检查IPS策略的配置信息。

```
<USG>dis ips policy test
    Signature set : test
     Direction   : to-server,to-client
     Severity    : >= warning
     Reliability : disable
     Protocol    : disable
     Category    : disable
     State       : enable
     Action      : block
     Override list(0):
     ID   Action    State     Name
     ----------------------------------------
```




- 检查签名集是否包含该攻击的签名，如果不包含，尝试调整方向、严重性、协议等参数后再次查看是否包含该攻击的签名。如果有特权策略，则相应的检查特权策略中是否包含该攻击的签名。

to-server、to-client指的是报文的方向，如HTTP的请求报文，就是to-server，HTTP的回应报文就是to-client的。对于UDP协议，谁先发报文，谁就是client端，发出去的报文为to-server。

当所有选项都没有“开启”时，表示该签名集包含了所有签名。当有选项开启了但没有指定具体的值，则该签名集不包任何签名。

签名集（包括模板中的签名集）之间存在优先关系，在同一条IPS策略中，排在前面的签名集比排在后面的签名集的优先级高。如果一个签名包含在一条IPS策略的多个签名集中，则USG按照优先级高的签名集所配置的启用状态和响应方式对匹配签名的报文进行处理

自定义签名只能通过覆盖签名的方式加入到策略中。



原因一：配置问题

- 执行命令ips configure commit，对IPS策略进行编译。

```
[USG]ips configure commit
05:57:10  2008/09/16
Info: No configuration need to commit.
```


- 如果显示提交成功则说明之前未提交过，显示不需要提交说明之前已经做过提交。
- 修改已应用在域间的IPS策略的签名或覆盖签名的配置后，这些修改不会立即生效，需要使用ips configure commit命令提交配置，更新IPS策略。
- 与IPS策略相关的以下修改需要提交编译后才生效：
  - 增加、删除、修改签名；
  - 增加、删除、修改覆盖签名；
  - 删除、修改自定义签名。

原因二：引擎及特征库问题

- 执行命令display ips version，查看当前设备是否已加载IPS特征库及引擎。

```
[UTM5000_A]display ips version
06:21:08  2008/09/16
=================Update information list===================
 Current version :
 Version number               : 20090827.009
 Engine version               : 4.002
 Engine size                  : 1204020 bytes
 Signature database version   : 20090827.009
 Signature database size      : 622569 bytes
 Update time                  : 02:52:10 2008/09/16
 Issue time of the update file : 17:56:07 2009/08/27
==============================================================
```




- Current version表示当前版本的IPS特征库及引擎版本信息。如果Current version没有或者该版本不是最新发布版本，请检查升级问题，如果检查配置都正确，特征库及引擎版本都是最新版本，如果还不能检测该攻击，则有可能是新型攻击，不能识别，请联系技术支持。



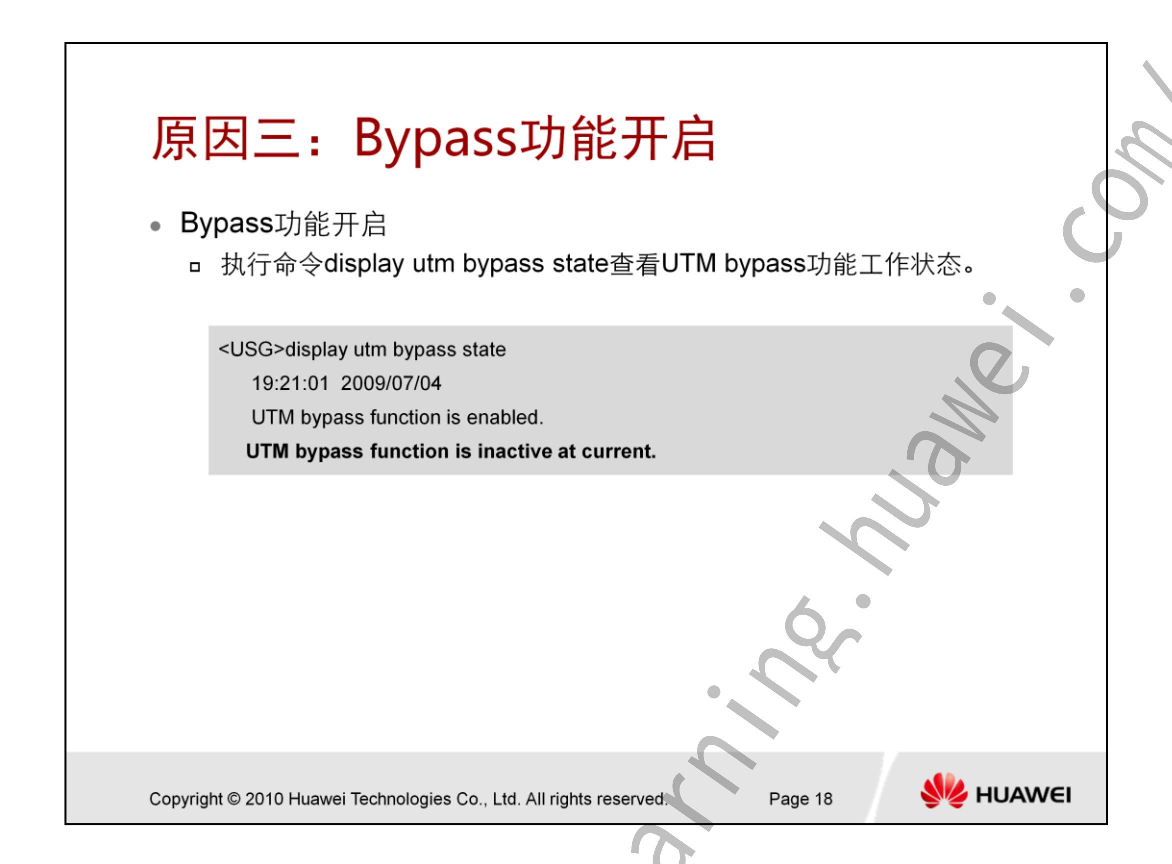
原因二：引擎及特征库问题

- 执行命令display license，查看License是否过期。

```
[UTM5000_A]display license
06:33:39  2008/09/16
Device ESN is: 2102351337Z08C000032
Have already activated 1 License file,the file is:
flash:/on1032318.dat    Activated time: 2008/08/13  09:21:08
VPN          : 7000
VFW          : 50
GTP          : ENABLED
IPS          : ENABLED;  Expiration date: 2010-04-15
URL Filter   : ENABLED;  Expiration date: 2008-12-15
Anti Virus   : ENABLED;  Expiration date: 2010-04-15
```

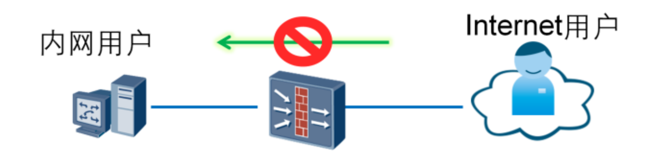



- 临时license存在使用期限，商用license永久有效，但升级服务有时间限制，如果版本不能更新，可以查看升级服务是否到期。



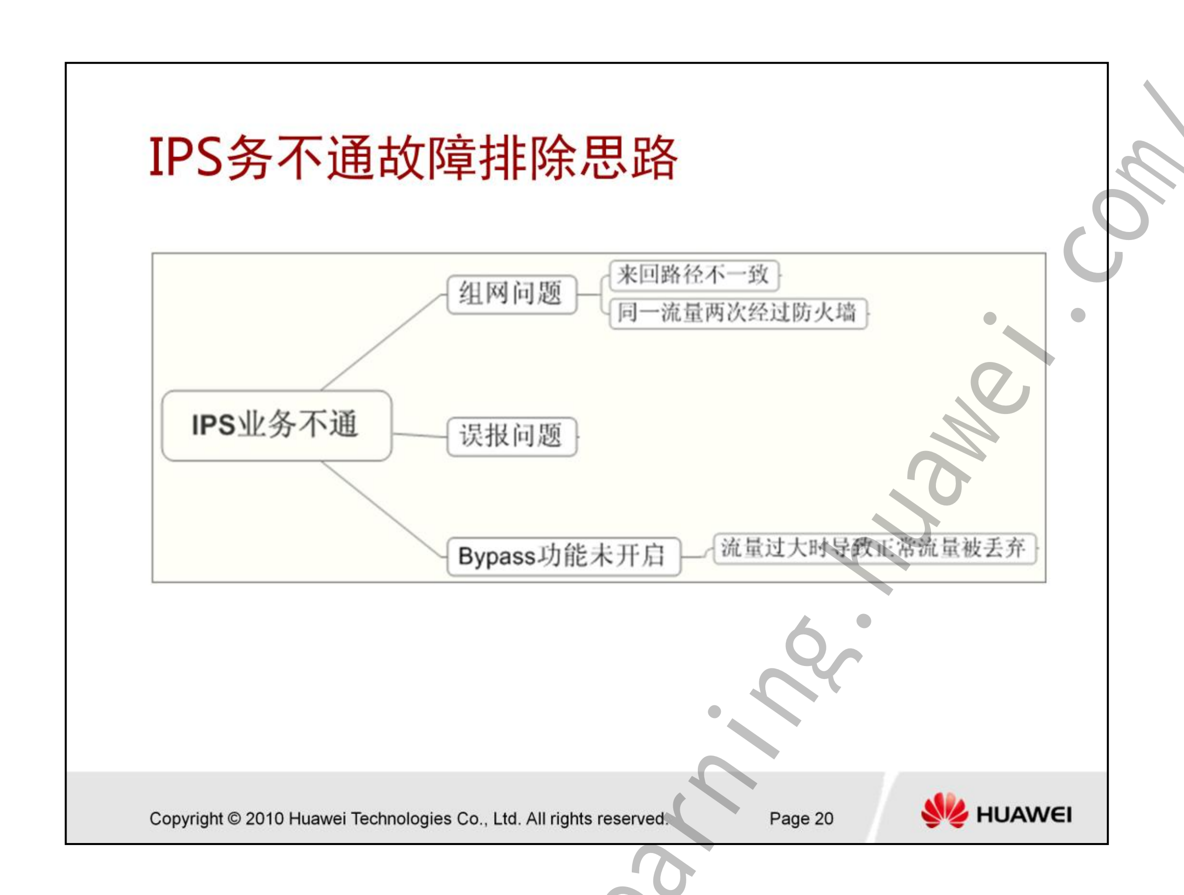
- 当处理能力不足时,为了保证用户体验,USG会优先选择放行业务,不做检测Inactive 表明utm没有bypass,Active表明发生了bypass。

IPS业务不通故障排除

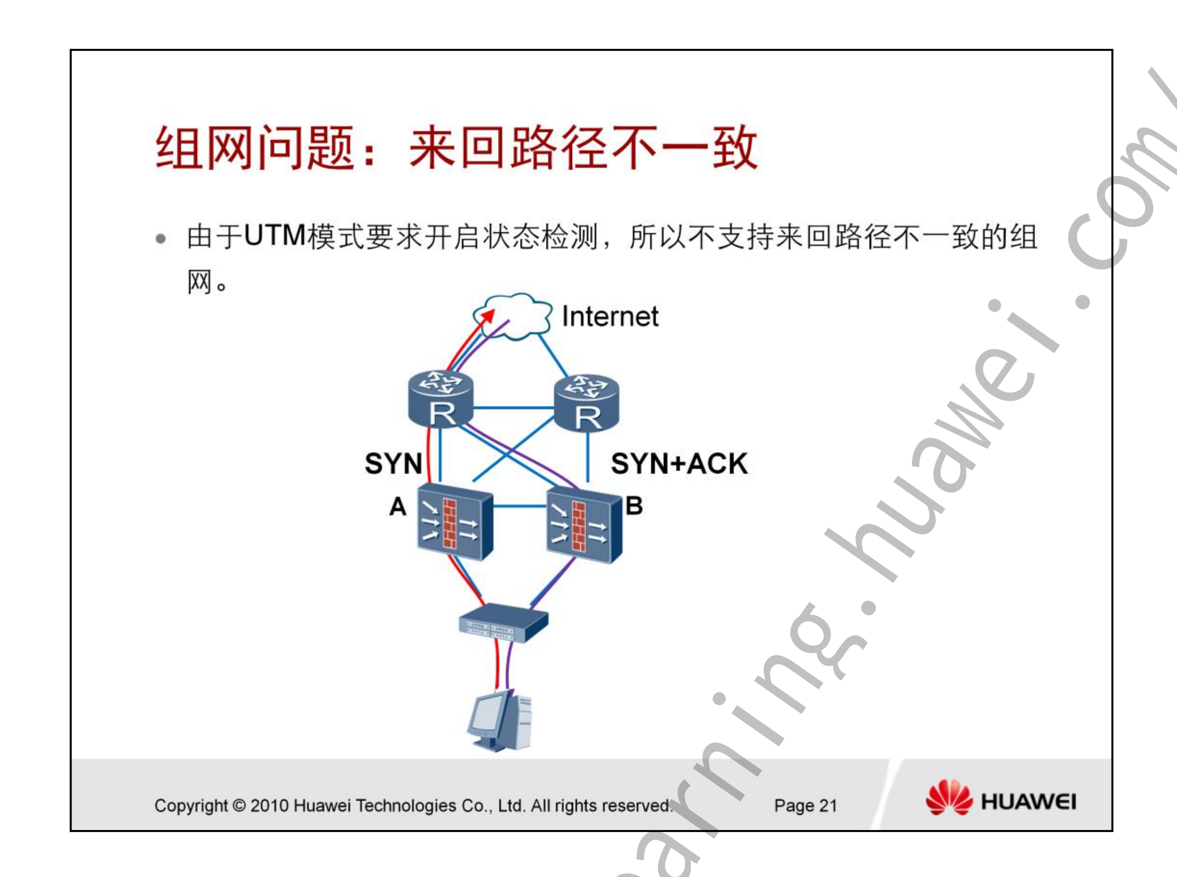


- 现象描述
  - 开启IPS功能后，配置正确的情况下，某些需要通过防火墙的业务不通，即IPS业务不通。



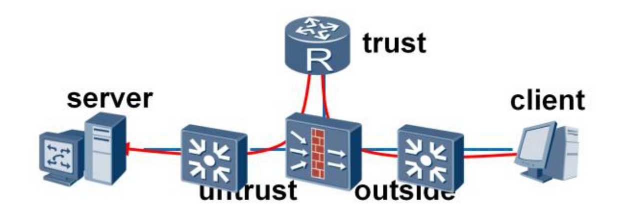


- 当网络上出现流量不通或部分业务不通，如游戏经常断线之类的网络故障时，可通过以上步骤来快速判定是否是IPS模块的问题并尽可能的解决问题。



- 三次握手的报文经过两个不同的路径:客户端发出的syn报文经过防火墙A，而服务器返回的syn+ack报文却经过防火墙B返回给客户端，这时防火墙B收到该报文却找不到会话，会把该报文丢弃，客户端无法完成三次握手。而防火墙A会因为收不到syn＋ack报文导致流程中断，后续业务不正常。

组网问题：同一报文两次经过防火墙



- 故障描述
  - 防火墙工作在透明模式或混合模式，开启UTM功能（IPS、AV或URL过滤），业务报文流行为outside→trust→untrust，两次经过防火墙，此场景下会导致HTTP/SMTP/POP3或其他业务不通。
- 解决方法
  - 调整网络，避免走UTM流程处理的业务两次经过防火墙；
  - 调整防火墙配置，两次经过防火墙业务不再进行UTM流程处理。



组网问题：同一报文两次经过防火墙

- 原配置

```
policy interzone trust untrust inbound
 policy 0
 action permit
 policy ips protect_pc
 policy av protect_pc
#
policy interzone trust untrust outbound
 policy 0
 action permit
 policy ips protect_pc
 policy av protect_pc
```

```
policy interzone trust outside inbound
 policy 0
 action permit
 policy ips protect_pc
 policy av protect_pc
#
policy interzone trust outside outbound
 policy 0
 action permit
 policy ips protect_pc
 policy av protect_pc
```




组网问题：同一报文两次经过防火墙

- 修改配置解决法
  - 配置服务器和客户端地址集

```
[USG5000]ip address-set server type object
[USG5000-object-address-set-server]address 10.11.140.51 0
//服务器，IP地址根据实际情况做调整
[USG5000]ip address-set client type object
[USG5000-object-address-set-client]address 10.11.140.117 0
//客户端，IP地址根据实际情况做调整
```

  - 域间策略服务器和客户端互访不再进行AV/IPS检测处理



组网问题：同一报文两次经过防火墙

```
policy interzone trust untrust inbound
 policy 0
 action permit
 policy source address-set server
 policy destination address-set client
 policy 1
 action permit
 policy ips protect_pc
 policy av protect_pc
#
policy interzone trust untrust outbound
 policy 0
 action permit
 policy source address-set client
 policy destination address-set server
 policy 1
 action permit
 policy ips protect_pc
 policy av protect_pc
```

```
policy interzone trust outside inbound
 policy 0
 action permit
 policy source address-set client
 policy destination address-set server
 policy 1
 action permit
 policy ips protect_pc
 policy av protect_pc
#
policy interzone trust outside outbound
 policy 0
 action permit
 policy source address-set server
 policy destination address-set client
 policy 1
 action permit
 policy ips protect_pc
 policy av protect_pc
```




IPS业务不通故障排除步骤

- 检查组网是否存在来回路径不一致或者同一报文两次经过防火墙的情况。
- 判断是否是误报，需要分析流量，如无法确定，可抓包发给技术支持人员分析。如果确定为误报，执行步骤3。
- 找到该流量所用的IPS策略，可利用覆盖签名去使能该签名或把该签名的动作改成alert。 undo override-signature id enable
- 系统视图执行 display utm bypass state 查看utm bypass功能是否开启，disable表示未开启，通过命令utm bypass enable开启该功能。
- 如果上述方法不能排除故障，可以尝试步骤5、6。
- 修改ips策略并执行命令ips configure commit将IPS策略提交编译。
- 执行命令update online ips升级IPS特征库库。



- 可以通过查看日志判断是否产生IPS攻击，再看动作是否为block,还要判断该日志是否针对问题流量的。
- IPS会话或NDC会话满规格后，若没有开启流量bypass功能，会阻断超过规格的流量
- 我们可通过修改策略来触发状态机的重新编译。如把策略中的某条签名的动作由block改成alert再改成block。这样配置没有真正改变，但执行ips configure commit 还是会重新编译状态机。若出现 “Info: No configuration need to commit.” 则表示没有编译状态机。
- 升级特征库主要是解决引擎的错误。



目录

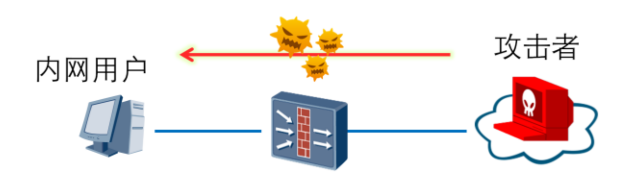


AV配置注意事项

- HTTP加速传输体验的开启可能造成页面不能推送，或者放过病毒但关闭可能造成在线视频应用连接时间较长。
- 建议开启断点续传检测功能。
- 仅配置支持热备，而病毒引擎和病毒库不支持。



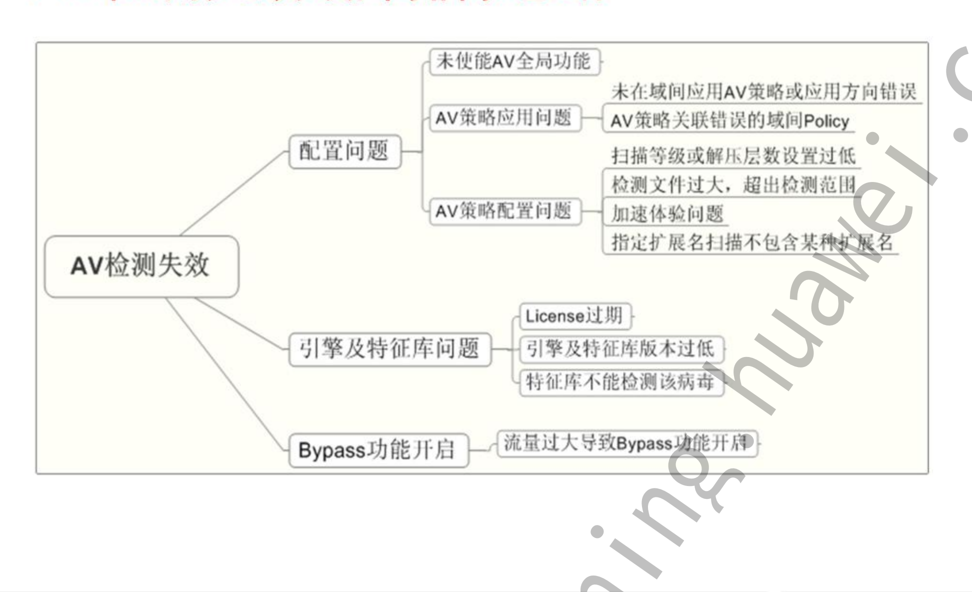
AV检测失效故障排除



- 现象描述
  - 防火墙开启AV功能后，不能检测到病毒。



AV检测失效故障排除思路





HUAWEI

原因一：配置问题

- 未使能AV全局开关
  - 执行命令display av global-configuration，查看av全局开关使能状态。

```
Anti-Virus Global Configuration Info
------------------------------------------------------------
      Anti-Virus global switch :     Enable
      Scan level              :      2
      Max decompressable layer :      10
```




查看av全局开关使能状态：如果状态为enable，表示使能。如果状态为disable，表示未开启。扫描等级取值越高，病毒检测率会越高，但产生误报的可能性也越大。当网络上传输的文件的压缩层数小于或等于最大解压层数时，文件将被解压，然后进行扫描；当文件的压缩层数大于最大解压层数时，不对文件进行扫描，并按照超过最大解压层数的动作处理。

原因一：配置问题

- AV策略应用问题
  - 执行命令dis policy interzone zone1 zone2 {inbound | outbound}，查看用户与Internet所属的域间是否应用了AV策略，策略应用的方向及关联的Policy是否正确。

```
policy interzone trust untrust outbound
    policy 0
     action permit
     policy av ggg
    policy 1
     action permit
     policy service service-set ip
     policy source any
     policy destination any
     policy av abc
```




- 应用AV策略时，要注意：
  - 方向问题，是会话发起的方向；
  - 关联policy时，policy是顺序匹配，匹配到一条后不再往下匹配。

原因一：配置问题

- AV策略配置问题
  - 执行命令display av policy，查看av策略配置。

```
<USG> display av policy
========================================
    Public Confirutarion
========================================
Policy name                   :  av-policy
Description                   :  Anti-Virus policy
Use reference                 :  0
Password-protected-file action  :  Permit
Deep-compressed-file action     :  Permit
Large-file action               :  Permit
========================================
    HTTP Protocol
========================================
HTTP switch                   :  Enabled
Action                        :  Block
Action when over-load         :  Bypass
Max file size to scan         :  10 MBytes
Web push notification         :  Warning: the page you request includes virus
```


HUAWEI

- AV策略配置中容易导致AV检测失效的参数有：
  - 超大文件，最大处理能力为20M，超大文件参数设置为允许则超过20M文件直接放行；
  - 超过解压层数文件，参数设置为允许，则超过解压层数的文件直接放行；
  - 密码保护及受损文件，设置为允许，不能检测直接放行；
  - HTTP加速体验会导致检测能力受影响；
  - 指定扩展名扫描中不包含某种扩展名。

原因二：引擎及特征库问题

- 引擎及特征库问题
  - 执行命令display av version，查看是否已加载AV引擎及签名库。

```
Current version :
  Version number                : 20090811.001
  Engine version                : 1.000
  Engine size                   : 2008792 bytes
  Signature database version    : 20090811.001
  Signature database size       : 48057345 bytes
  Update time                   : 18:41:13 2009/08/11
  Issue time of the update file : 02:32:24 2009/08/12
```



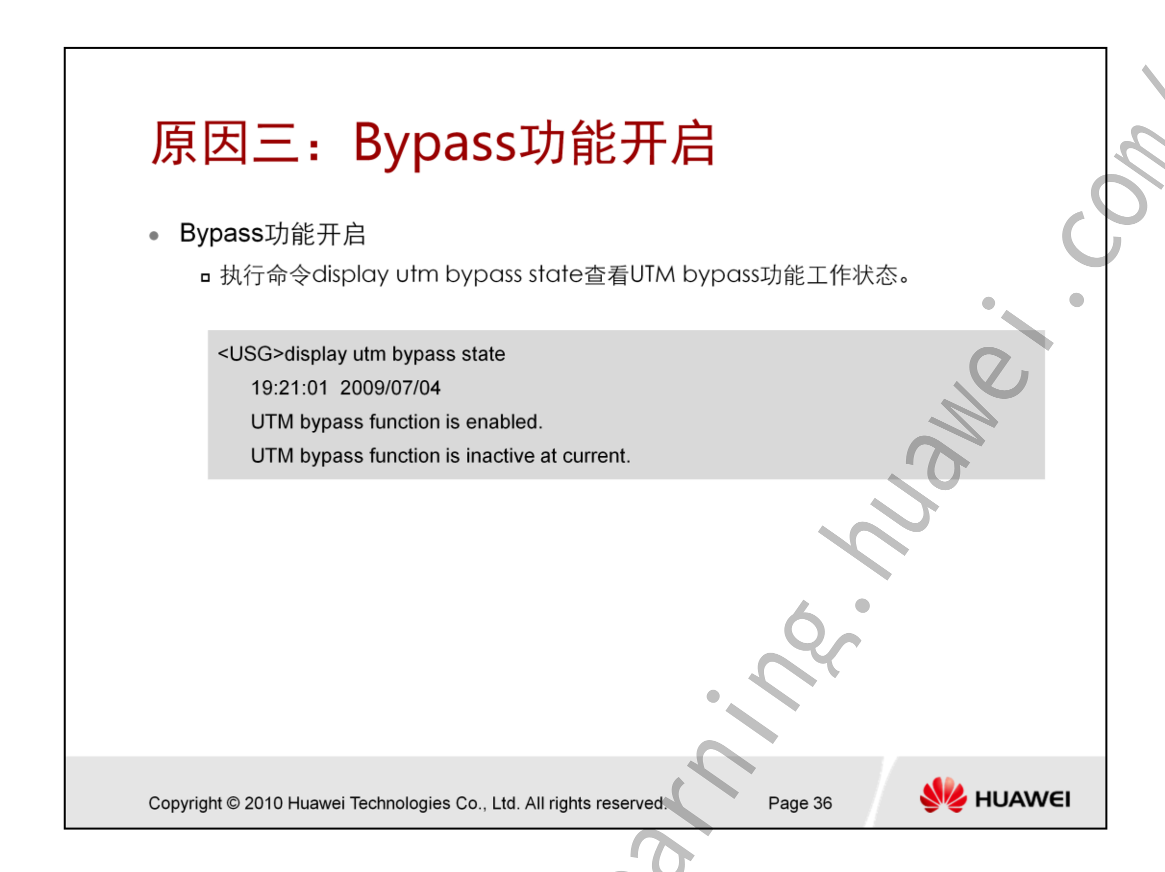

- Current version表示当前版本的AV引擎及签名库版本信息。如果Current version没有或者该版本不是最新发布版本，请检查升级问题。如果版本为最新版本，配置正确的情况下，还是无法检测某些病毒，有可能是新的病毒不能检测，请联系技术支持。

原因二：引擎及特征库问题

- 执行命令display license，查看License是否过期。

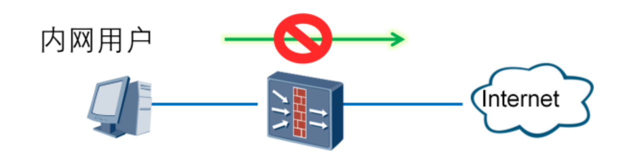
```
[USG2200]display license
06:33:39  2008/09/16
Device ESN is: 2102351337Z08C000032
Have already activated 1 License file,the file is:
flash:/on1032318.dat    Activated time: 2008/08/13  09:21:08
VPN          : 7000
VFW          : 50
GTP          : ENABLED
IPS          : ENABLED;  Expiration date: 2010-04-15
URL Filter   : ENABLED;  Expiration date: 2008-12-15
Anti Virus   : ENABLED;  Expiration date: 2010-04-15
```



- 当处理能力不足时,为了保证用户体验,USG会优先选择放行业务,不做检测Inactive 表明utm没有bypass,Active表明发生了bypass。

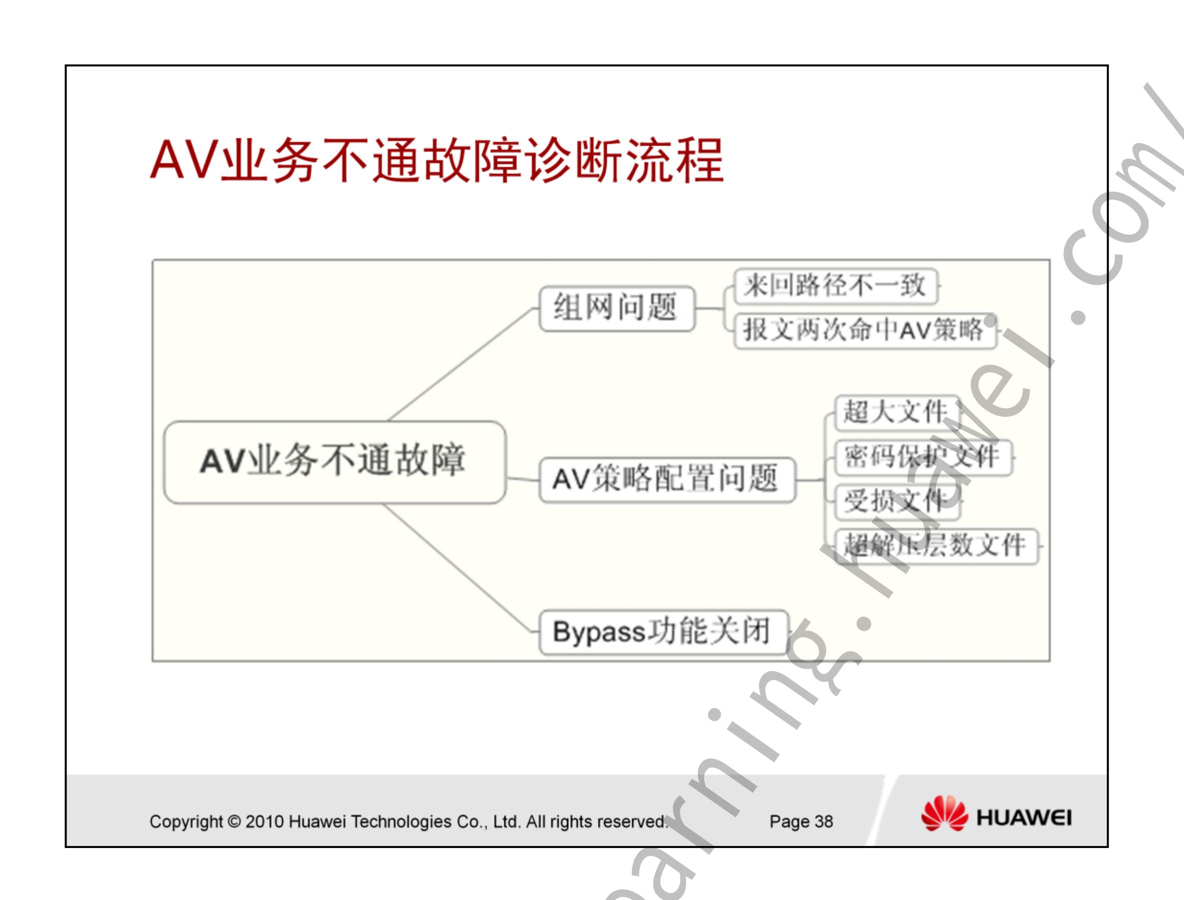
AV业务不通故障处理



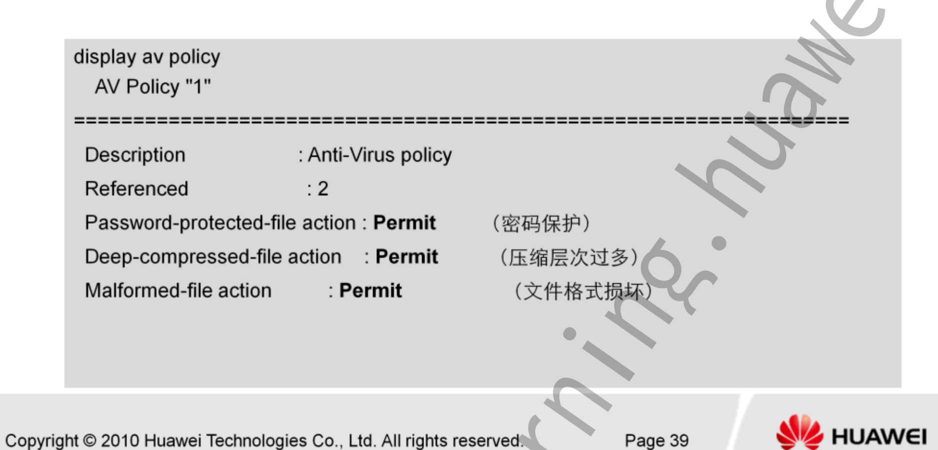
- 现象描述
  - 开启AV功能后，某些经过防火墙的上层的应用不通。如邮件不能发送或接收，HTTP网页不能正常浏览。



- Tcp代理的存在会改变报文序列号，如果和网络上其它设备结合，可能出现问题。由于AV特性使用的是全代理模型而非单纯的转发模型，因此某些应用场景下会造成业务不通。另外，网络上的其它设备的不当处理，也可能对AV业务造成影响，造成业务不通。AV业务对于以下两种应用场景不支持：来回路径不一致、报文两次命中av策略。
- 业务不通一般都是由于tcp连接时三次握手建立出现问题，需要依赖抓包和debug信息来定位。



- 当上层的应用不通。如邮件不能发送或接收，HTTP网页不能正常浏览，病毒文件不能正常扫描。可通过以下步骤来快速判定是否是AV模块的问题并尽可能的解决问题。（前提：配置都是正确的）



- 对于大文件、密码保护、文件格式损坏、压缩层次过多等情况，AV扫描引擎无法完成正常扫描，建议配置为permit。如果是deny可能导致业务失败，比如无法上传邮件附件等。

AV业务不通故障排除步骤

- 在视图执行命令display utm bypass state查看bypass状态 。

```
[USG5360]dis utm bypass state
16:44:33  2011/07/20
 UTM bypass function is disabled.
 UTM bypass function is inactive at current.
```




当流量过大，如果未开启UTM bypass功能，可能会因为性能不足导致部分业务问题。Disable表示未开启，通过命令utm bypass enable开启bypass功能。



目录



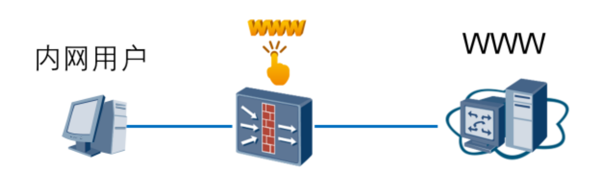
URL过滤配置注意事项

- 以下操作需要执行命令url-filter configure commit更新配置后才能生效。
  - 添加、删除黑白名单
  - 修改黑白名单的匹配方式
  - 修改黑白名单的匹配内容
  - 修改自定义分类的匹配方式
  - 修改自定义分类的匹配内容
  - 修改策略中自定义分类的动作
  - 添加或者删除自定义分类
- 如无高安全性等特殊需求，不建议配置查询预定义分类失败的动作为阻止，否则，由于网络状况不好等原因导致查询失败，将有可能造成用户的普通 HTTP访问失败。



用户更新配置后，由于设备会重新编译配置信息，对性能会有一定程度的影响。建议用户在完成所有配置后统一提交。

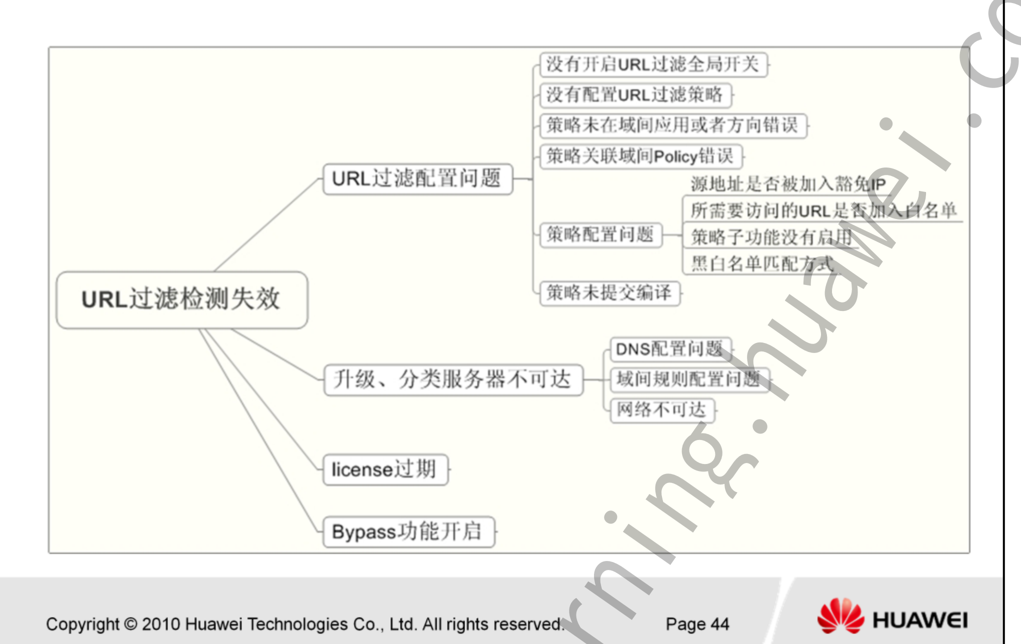
URL过滤失效故障排除



- 现象描述
  - 企业内网用户上网时，URL过滤功能失效。例如：某个URL已经加入黑名单，但用户仍然可以访问；某类URL的控制动作配置为阻止，但用户仍然可以访问。



URL过滤失效故障排除思路



HUAWEI

原因一：URL过滤配置问题

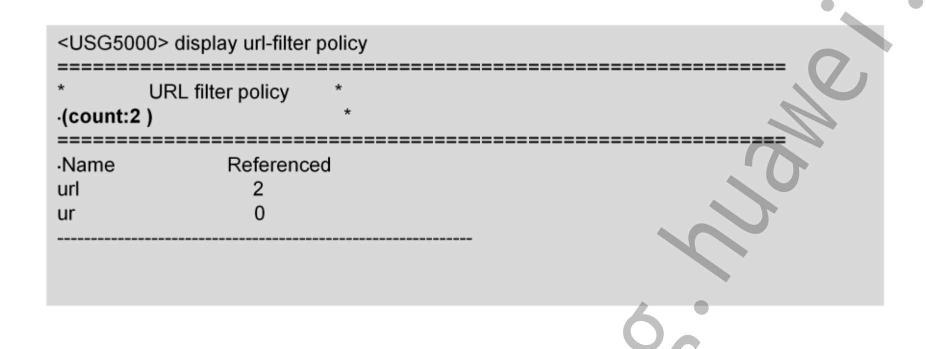
- URL过滤配置问题
  - 执行命令display url-filter global-configuration，查看URL过滤全局开关状态。

```
<USG5000>display url-filter global-configuration Global configuration information about
URL filtering
------------------------------------------------------------
 URL filtering global switch : Enable
 Default action              : Permit
 Category query fail action  : Permit
 Notification message        : The URL is forbidden.
```




原因一：URL过滤配置问题

- 执行命令display url-filter policy，查看URL过滤策略的配置。



```
<USG5000> display url-filter policy
=================================================================
*              URL filter policy        *
(count:2 )                               *
=================================================================
Name                    Referenced
url                        2
ur                         0
--------------------------------------------------------------
```

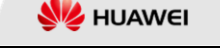



- 如果count为0，表示未配置URL过滤策略。

原因一：URL过滤配置问题

- 执行命令display policy interzone zone-name1 zone-name2 { inbound | outbound }，查看域间是否应用URL过滤策略。

```
<USG5000> display policy interzone trust untrust outbound policy interzone trust
untrust outbound
 firewall default packet-filter is permit
 policy 0 (49 times matched)
  action permit
  policy service service-set ip
  policy source any
  policy destination any
  policy url-filter url
```

- 在该步骤中需要注意所配置的URL过滤策略方向与HTTP请求会话建立的方向是否一致。应该根据HTTP请求会话建立的方向决定URL过滤策略配置inbound还是outbound方向。另外需要注意关联正确的policy，policy是按顺序执行。

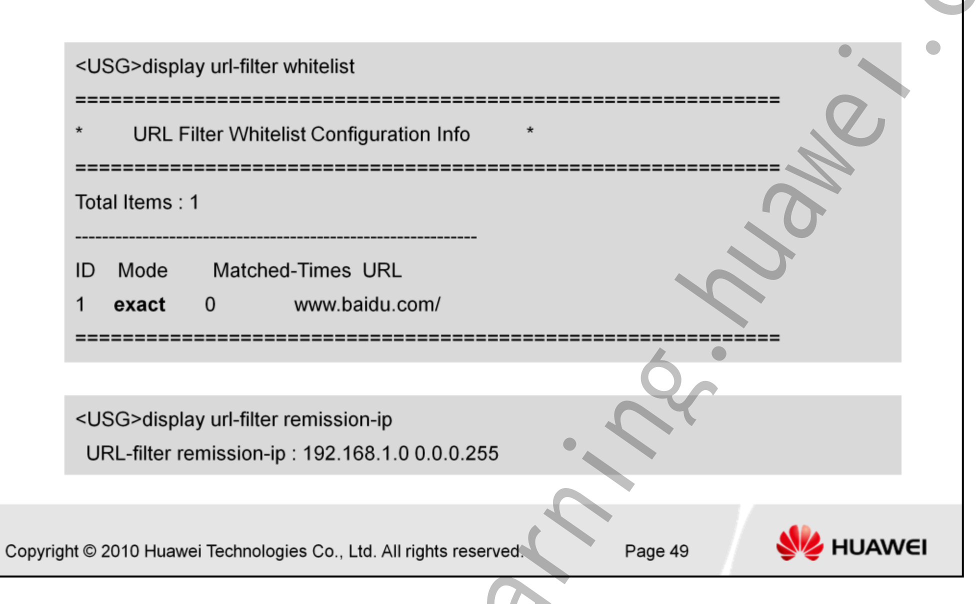
原因一：URL过滤配置问题

- 执行命令display url-filter policy policy-name，查看策略设置

```
<USG5000> display url-filter policy url
URL filter policy "url"
  Description           :
  Referenced            : 2
  Remission-IP          : Disable
  Blacklist             : Enable
  Whitelist             : Enable
  User-defined category : Enable
  Pre-defined category  : Enable
```




- 在策略设置中，要注意启用相应的功能，如配置了黑白名单，需要启用黑白名单，选择自定义分类或者预定义分类。
- 另外关于url的过滤顺序是按照：豁免ip、白名单、黑名单、自定义分类、预定义分类，跟sweb页面显示的顺序无关。
- url预定义分类里面专门有个分类叫other-sites，远程服务器里找不到分类的域名都归到这里。



- 检查失效的源地址是否被加到豁免ip地址中，失效的目标是否被加入到白名单，或者被加入到黑名单中，但由于匹配方式设置不当导致黑名单没有匹配上。如设置黑名单精确匹配www.baidu.com但是还是可以打开mp3.baidu.com。



如果提示信息为“Info: Commit successful.”，说明配置提交成功。

如果提示信息为“Info: No configuration need to commit.”，说明没有需要提交的配置。

原因二：升级、分类服务器不可达

- DNS设置问题
  - 执行命令display dns dynamic-host，查看动态域名解析缓存信息是否解析到分类服务器地址。

```
<USG> display dns dynamic-host
No Domain-name IpAddress TTL
```

  - 执行命令display dns resolve，查看是否开启DNS解析功能。

```
<USG5000> display dns resolve
 DNS resolve is disabled.
```

  - 执行命令display dns server，查看DNS地址配置是否正确。

```
<USG5000> display dns server
 IPv4 Dns Servers :
 No configured servers.
```




使用预定义分类策略的时候，防火墙需要在线查询预定义分类服务器，使用的是域名方式，需要防火墙开启DNS功能，如果未开启DNS功能则首先开启DNS功能。然后检查DNS服务器地址是否设置正确，DNS服务器是否可用。

原因二：升级、分类服务器不可达

- 域间规则设置问题
  - 执行命令display policy interzone local untrust outbound检查防火墙到外网域间规则是否开启。

```
[USG]dis policy interzone local untrust outbound
policy interzone local untrust outbound
 firewall default packet-filter is permit
```

- 网络不可达
  - 执行命令display security server，查看USG与安全服务中心是否已连接.

```
<USG> display security server
 Security server : sec.huawei.com
 URL Filter Connection State : 1(0-Disconnected 1-Connecting 2-Connected)
```

  - 在排除DNS和域间规则问题后，请检查网络问题。



使用预定义分类策略时，防火墙需要与分类服务器通讯，因此要开启防火墙到外网域间规则。



原因三：License不存在或失效

- 执行命令display license，查看License是否不存在或者过期。

```
<USG5000> display license
Device ESN is: 2102351337Z08C000025
Have already activated 1 License file, the file is:
cf:/on1032318.dat    Activated time: 2009/09/01 15:59:47
flash:/ON1032318.dat  Activated time: 2009/09/11 15:58:35
flash:/license.dat    Activated time: 2009/09/29 19:44:35
VPN          : 7000
VFW          : 50
GTP          : ENABLED
IPS          : ENABLED;  Expires: 2010-09-02
URL Filter   : ENABLED
Anti Virus   : ENABLED;  Expires: 2011-09-02
```




- 正式商用license永久有效，显示过期时间为“expire time:9999-12-31”，临时license一般有效期为三个月。

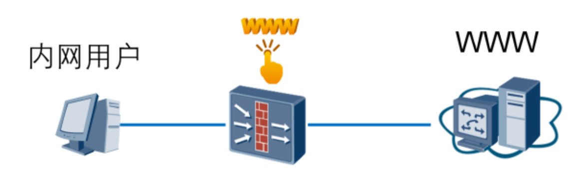
原因四：Bypass功能开启

- Bypass功能开启
  - 如果客户反映url功能有时生效有时不生效，重点怀疑是否是流量过大造成。
  - 特别注意是否同时开启了其它UTM业务，流量过大导致bypass功能开启。

```
[USG]display  utm bypass state
UTM bypass function is enabled.
UTM bypass function is active at current.
```




URL过滤故障排除案例



- 故障描述
  - 用户启用了url过滤功能，激活licence后，配置了黑白名单，预定义策略和自定义策略，都不生效，无一条匹配上应用的策略，如右图所示。

```
[USG2200]disp url-filter statistics
19:26:34  2011/08/08
Statistic information about URL filtering
-----------------------------------------------------------
 Total HTTP requests            : 0
 Total permitted HTTP requests : 0
 Total denied HTTP requests    : 0
 Match blacklist               : 0
 Match whitelist               : 0
 Match user-defined category   : 0
 Match pre-defined category    : 0
 Default action                : 0
```



URL过滤故障排除案例

- 定位步骤
  - 检查url过滤功能的license激活并在有效期内；
  - 检查防火墙模式为UTM，检查url每个步骤配置，必配部分均以 配置，并在正确的域间应用了策略；
  - 细检查域间的策略发现policy 1 有命中，而policy2无一命中。

```
USG2200]disp policy interzone trust untrust outbound
policy interzone trust untrust outbound
 firewall default packet-filter is permit
 policy 1 (316123 times matched)
  action permit
  policy url-filter worktime
  ……
 policy 2 (0 times matched)
  action permit
  policy url-filter worktime
```




策略只要命中一个就不会再执行剩下的策略，所以需要把所有的UTM的功能都加到一个策略里面。



目录

1. UTM故障排除
2. IPS故障排除
3. AV故障排除
4. URL过滤故障排除
5. **RBL过滤故障排除**
6. 上网行为管理故障排除
7. 升级网站故障排除



RBL过滤注意事项

- DNS服务器用来查找RBL服务器，只有配置了用于查询RBL的DNS服务器，USG才能与RBL服务器建立连接。
- 选择DNS服务器时需要注意： 必须使用没有被DNS劫持的DNS服务器，否则所有发送邮件的源IP地址，都会被认为列入到了RBL中，用户将接收不到任何外部邮件。
- 由于RBL过滤的匹配顺序为：本地白名单、本地黑名单、远程黑名单，所以请确保白名单中没有列入垃圾邮件的源地址，否则即使在远程黑名单中有该地址，邮件不能过滤。

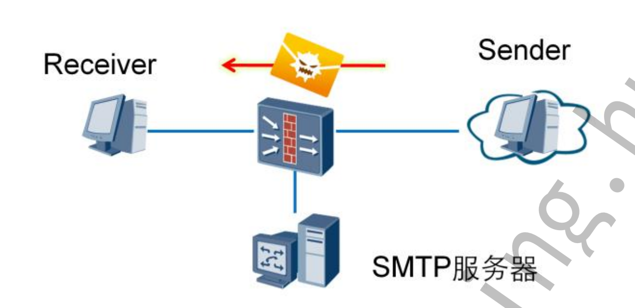


DNS劫持是指服务提供商为引导用户访问其增值站点或合作站点，对DNS服务器做修改，在接收到一个不存在结果的DNS查询时，总是返回一些特定的IP地址，使用户访问到这些增值站点。

必须使用可以进行递归查询的DNS服务器，而不是进行迭代查询的DNS服务器。

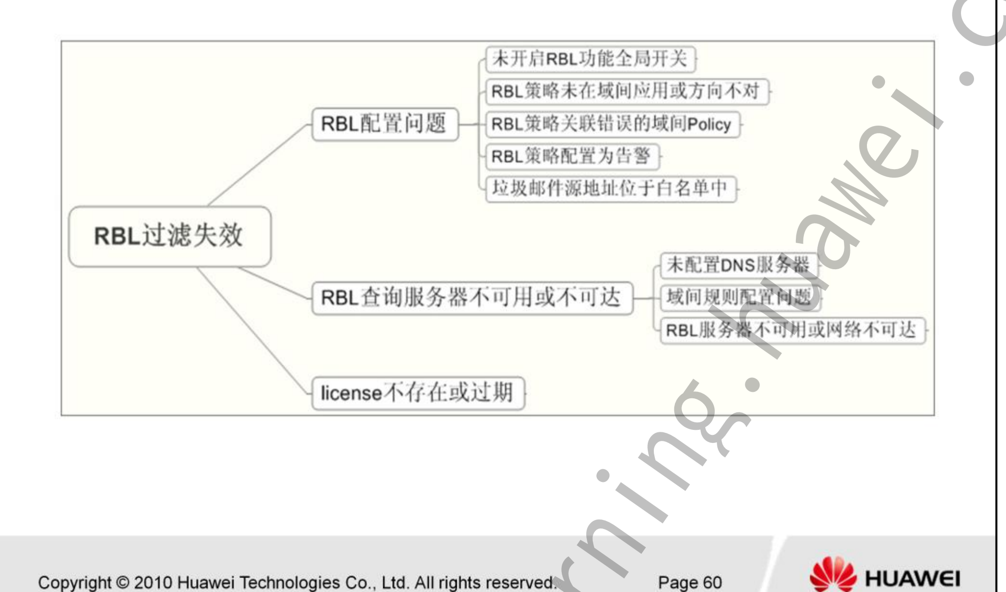
RBL过滤故障排除

- 现象描述
  - 开启了RBL过滤功能，但是用户还是收到大量垃圾邮件，RBL过滤功能失效。





RBL过滤故障排除思路



HUAWEI



原因一：RBL配置问题

- 执行命令display rbl-filter global-configuration，查看RBL过滤的启用状态。

```
<USG> display rbl-filter global-configuration
------------------------------------------------------------
 RBL filter               : Enable
 RBL enabled profile      : Pre-define
 RBL server IP address    : 192.168.1.10, 192.168.1.11
 RBL whitelist            : Enable
 RBL blacklist            : Disable
------------------------------------------------------------
```




注意RBL功能已经黑白名单功能是否开启，使用的是自定义的RBL过滤策略还是预定义的RBL过滤策略。

原因一：RBL配置问题

- 执行命令display policy interzone zone1–name zone2–name { inbound | outbound }，查看域间是否应用RBL过滤策略，方向及关联的策略是否正确。

```
<USG> display policy interzone dmz untrust inbound
policy interzone dmz untrust inbound
 firewall default packet-filter is permit
 policy 0 (49 times matched)
 action permit
 policy service service-set ip
 policy source any
 policy destination any
 policy rbl-filter
```




只有匹配防火墙策略并允许通过的数据流才会进行RBL过滤。注意RBL策略应用的方向。同一个域间防火墙策略视图下可配置多个防火墙策略。缺省情况下，越先配置的策略，优先级越高，越先匹配报文。

原因一：RBL配置问题

- 执行命令display rbl-filter pre-define，查看RBL预定义策略配置。

```
<USG> display rbl-filter pre-define
Pre-define Profile
==============================================================
Switch       : Enable
Action       : Alert
Description  : Use the default symantec's RBL server.
==============================================================
```


如果为Alert，那么即使垃圾邮件匹配到远程黑名单，还是照常转发，如果希望拒绝垃圾邮件，请将动作设置为block。

原因一：RBL配置问题

- 执行命令display rbl-filter whitelist，查看本地白名单的具体信息。

```
<USG> display rbl-filter whitelist
=========================================================
RBL whitelist(2):
IP address      Mask
---------------------------------------------------------
10.17.1.0      255.255.255.0
1.1.1.0        255.255.255.0
=========================================================
```




由于RBL过滤的匹配顺序为：本地白名单、本地黑名单、远程黑名单，所以请确保白名单中没有列入垃圾邮件的源地址，否则即使在远程黑名单中有该地址，邮件不能过滤。

原因二：RBL服务器不可用或不可达

- 执行命令display rbl-filter global-configuration，查看DNS服务器的IP地址。

```
<USG> display rbl-filter global-configuration
------------------------------------------------------------
 RBL filter              : Enable
 RBL enabled profile     : Pre-define
 RBL server IP address   : 192.168.1.10, 192.168.1.11
 RBL whitelist           : Enable
 RBL blacklist           : Disable
------------------------------------------------------------
```




必须使用没有被DNS劫持的DNS服务器，否则所有发送邮件的源IP地址，都会被认为列入到了RBL中，用户将接收不到任何外部邮件。

DNS劫持是指服务提供商为引导用户访问其增值站点或合作站点，对DNS服务器做修改，在接收到一个不存在结果的DNS查询时，总是返回一些特定的IP地址，使用户访问到这些增值站点。

原因二：RBL服务器不可用或不可达

- 执行命令display policy interzone local untrust outbound，查看local到外网域间规则设置。

```
[USG5560]display policy interzone  local untrust outbound
policy interzone local untrust outbound
 firewall default packet-filter is permit
```

- 检查DNS服务器、RBL服务器网络可达性。



- 不回复应答码或回复的应答码未在USG上配置的情况下，放行邮件。

原因三：License不存在或过期

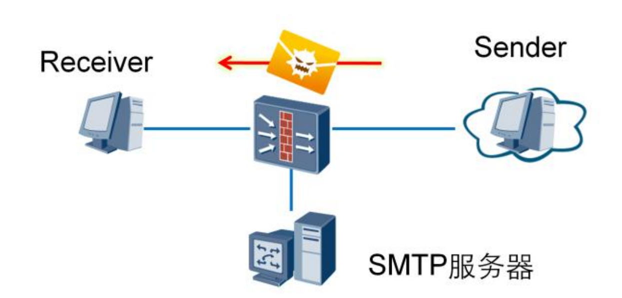
- 执行命令display license，查看license情况。

```
[USG]display license
16:49:27  2011/12/02
Device ESN is: 210235G6HUZ0B6000028
The file activated is: hda1:/lic6047002844-aa68d3058e1_usg5560.dat
The time when activated is: 2011/09/30  18:02:39
IPS: ENABLED
expire time:9999-12-31.
Anti Virus: ENABLED
expire time:9999-12-31.
URL Filter: ENABLED
expire time:9999-12-31.
Anti Spam: ENABLED
expire time:9999-12-31.
```




License不存在或者过期，将无法使用预定义的RBL过滤。

案例：DNS劫持导致接收不到任何邮件



- 现象描述
  - 用户接收不到任何外部邮件。
- 可能原因
  - 所有发送邮件的源IP地址，都会被认为列入到了RBL中，配置的DNS服务器不能使用，是被劫持的。



案例：DNS劫持导致接收不到任何邮件

- 处理步骤
  - 使用RBL服务提供商提供的测试地址进行测试 使用RBL服务提供商提供的测试地址进行测试，预期结果为：返回的应答码与RBL服务提供商提供的应答码为一致。例如：cbl.anti-spam.org.cn提供的测试地址为2.0.0.127.cbl.anti-spam.org.cn，提供的应答码为127.0.8.2，要测试的DNS服务器为165.87.13.129；
  - 使用不属于远程黑名单的IP地址进行测试 1.1.1.1这个IP地址一般不会被列入远程黑名单，使用此IP地址进行测试。预期结果为：Non-existent domain。如果反馈的不是这个结果而是IP地址，表示该DNS服务器被劫持。



- 选择一个合适的DNS服务器IP地址，用于连接RBL服务器进行正确的查询。判断DNS服务器是否被劫持。根据RBL服务提供商提供的测试地址和不属于远程黑名单的地址分别进行测试，只有两个测试结果都符合预期，才表明DNS没有被劫持。



目录



应用控制故障排除思路

- 常见故障
  - 升级故障
    - 未配置DNS
    - 存储空间不足
    - 时间选择不合理
  - 配置问题
    - 协议选择错误
    - 阻断配置错误
  - 特殊配置问题
    - 关联识别配置错误
    - 全包监测配置错误

应用控制故障排除步骤

- 故障点一：升级故障
  - 未配置DNS：远程升级时，未配置DNS导致sec.huawei.com无法实现地址解析；
  - 存储空间不足：设备重启后，无SA知识库，原因为使用了update rule-base no-save（本地升级）进行升级，知识库在内存中运行，下次重启知识库内容丢失；
  - 时间选择不合理：选择业务量大的时间升级，会导致升级不成功。
- 故障点二：配置问题
  - 协议选择错误：目前的SA知识库支持21大类协议集，每大类协议集下有众多协议小类。具体限制某种网络流量，需与流量使用的协议相关联
  - 阻断配置错误：匹配协议后，需要执行阻断策略，阻断策略需要在标准ACL中进行定义。



应用控制故障排除步骤

- 故障点三：特殊配置问题
  - 关联识别配置错误：对于多通道协议需要配置协议关联协议识别，如FTP、SIP、H.323等；
  - 全包监测配置错误：某些协议的报文是承载在其他协议上进行传输的，如MSN信息可能通过HTTP协议承载，此时需启用SA全包检测功能来支持此类报文的检测。



- 是否需要配置关联协议识别或全包监测，可以参考手册的“应用协议速查表”。

应用控制故障排除FAQ

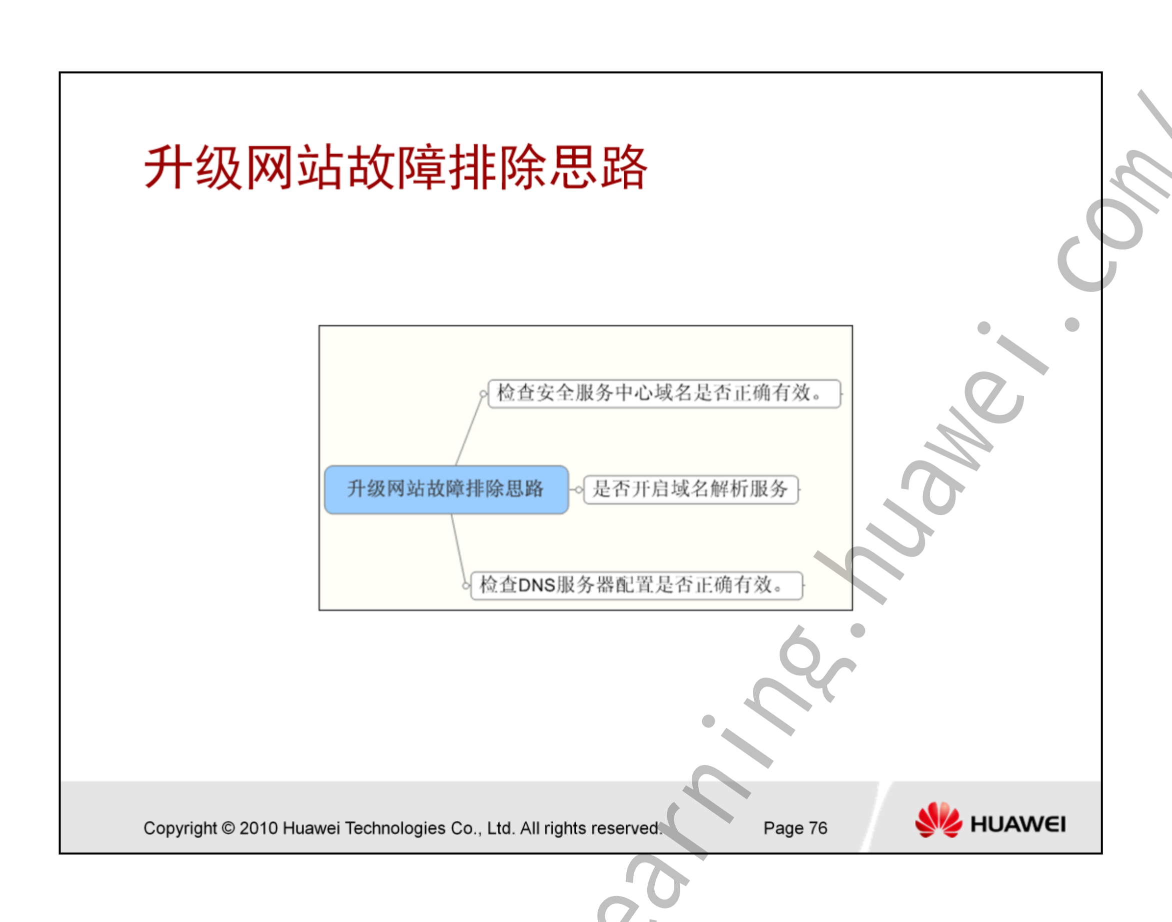
- FAQ-1：SA支持哪些类型协议的阻断及限流?
  - SA目前的特征文件版本支持21大类协议，每大类协议下有多种具体的协议：如：IM协议，下有QQ_IM、MSN_IM/MSN_Transfer、YahooMsg_IM等；具体情况请参考手册中的应用协议速查表。
- FAQ-2：刚安装后限流效果较好，运行一段时间限流效果不理想
  - 检查知识库文件不是最新，多种应用协议有过更新，知识库文件版本不是最新，导致协议匹配不上，限流效果不理想。一般情况下升级知识库版本可解决。
- FAQ-3：为什么知识库升级不成功?
  - 升级服务器域名或地址配置错误；
  - DNS 服务器未配置或配置错误；
  - 升级时间选择了业务高的时间，导致下载知识库文件失败；
  - 存储空间不足。





目录




升级网站故障排除思路
升级网站故障排除思路
检查安全服务中心域名是否正确有效。
是否开启域名解析服务
检查DNS服务器配置是否正确有效。
Copyright © 2010 Huawei Technologies Co., Ltd. All rights reserved.
Page 76
HUAWEI

升级网站故障排步骤

- 故障现象
  - USG可以访问Internet上的安全服务中心，在线升级IPS、AV的过程中，终端配置屏幕上出现以下提示信息。Error: Interacting with the security server error.
- 可能原因
  - 原因一：安全服务中心域名配置错误。
  - 原因二：未开启域名解析服务。
  - 原因三：DNS服务器的IP地址配置错误。



升级网站故障排步骤

- 处理步骤
  - 原因一：安全服务中心域名配置错误。
    - 执行命令display security server，查看安全服务中心域名配置信息。
  - 原因二：未开启域名解析服务。
    - 执行命令display current-configuration | in dns resolve，查看域名解析服务。
  - 原因三：DNS服务器的IP地址配置错误。
    - 执行命令display dns server，查看DNS服务器的IP地址。

 Page 78



- 原因一：安全服务中心域名配置错误。
  - 执行命令display security server 查看安全服务中心域名配置信息。
  - <USG> display security server Security server : sec.huawei.com URL Filter Connection State : 0(0-Disconnected 1-Connecting 2-Connected) Security server字段取值表示安全服务中心的地址。
  - 从显示信息可以看出，安全服务中心的域名为sec.huawei.com，请确认该域名是否正确。 如果正确，执行原因二。
  - 如果错误，在系统视图下执行命令security server domain domain-name重新配置。如果故障仍未排除，请执行原因二。
- 原因二：未开启域名解析服务。
  - 执行命令display current-configuration | in dns resolve 查看域名解析服务。
  - <USG> display current-configuration | in dns resolve dns resolve 如果输出没有包含 “dns resolve” 表示域名解析服务器未开启；如果输出包含 “dns resolve” 表示域名解析服务已开启。
  - 从显示信息可以看出，域名解析服务已经开启，请执行原因三，继续进行故障排除。
  - 如果DNS解析功能未启用，请启用。
  - 在系统视图下执行命令dns resolve 启用DNS解析功能。

  <USG> system-view [USG] dns resolve



总结

- UTM整体失效排查步骤?
- IPS常见故障排除思路及步骤?
- AV常见故障排除思路及步骤?
- URL过滤常见故障排除思路及步骤?
- RBL过滤常见故障排除思路及步骤?
- 应用控制常见故障排除及思路?
- 升级网站故障排除及步骤?



思考题

- 判断题
  1. 配置IPS签名集，当有选项开启了但没有指定具体的值，则该签名集包含所有签名。
- 多选题
  1. 与IPS策略相关的以下修改需要提交编译后才生效?

  A、增加、删除、修改签名

  B、增加、删除、修改覆盖签名

  C、删除、修改自定义签名

  D、在域间重新应用IPS策略



- 习题与答案:
  - 配置IPS签名集，当有选项开启了但没有指定具体的值，则该签名集包含所有签名

    答案：错误
  - 与IPS策略相关的以下修改需要提交编译后才生效?

    A、增加、删除、修改签名

    B、增加、删除、修改覆盖签名

    C、删除、修改自定义签名

    D、在域间重新应用IPS策略

    答案：A、B、C

Thank you

www.huawei.com

华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*) 享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：请提交您的“华为账号”和注册账号的“email地址”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训->面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见LVC排期：
    http://support.huawei.com/learning/NavigationAction!createNavi#navi[id]=_16
- **4、学习工具 eNSP**
  - *eNSP (Enterprise Network Simulation Platform),* 是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。（http://support.huawei.com/ecommunity/bbs/list_2247.html ）

